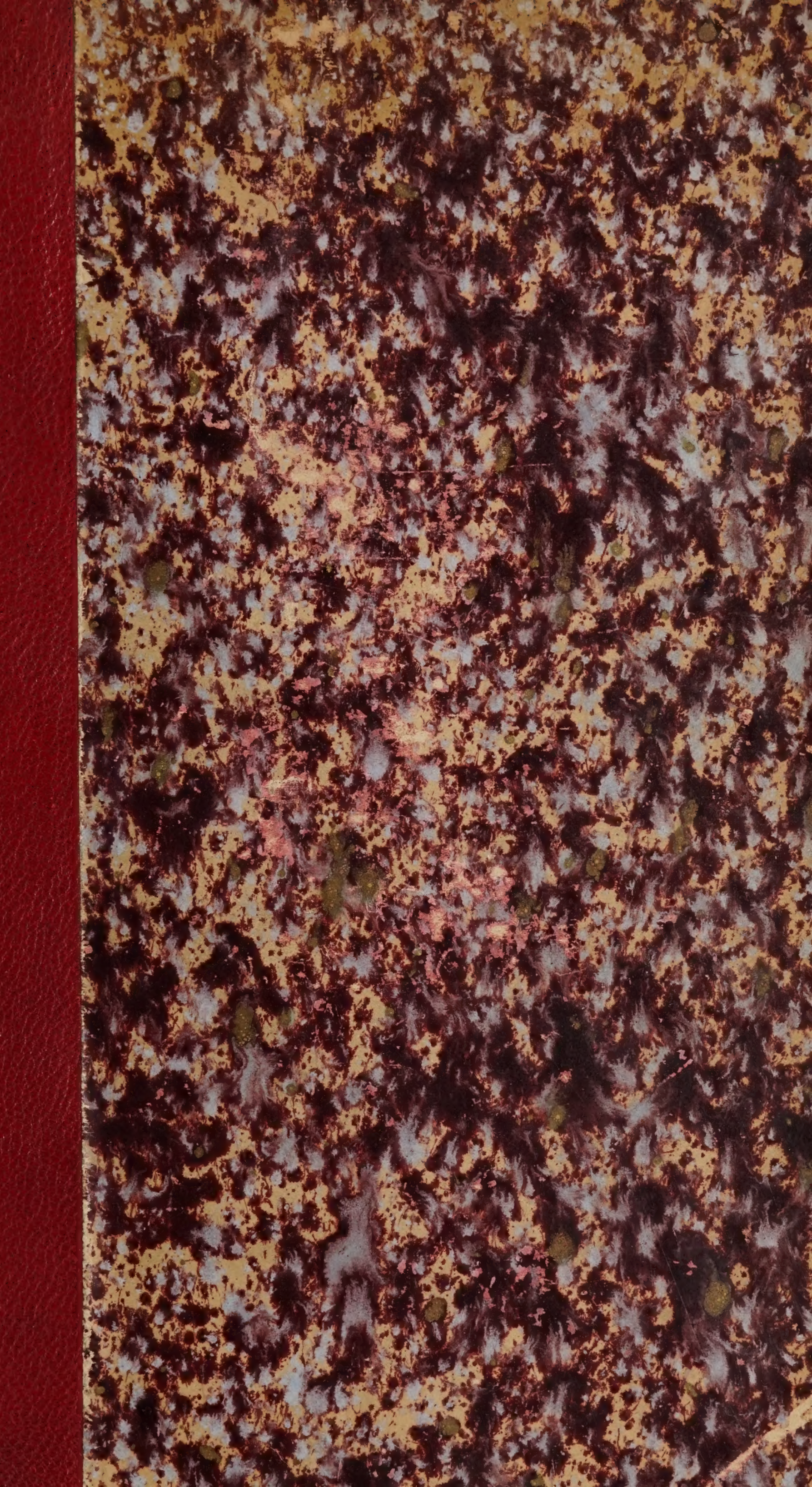
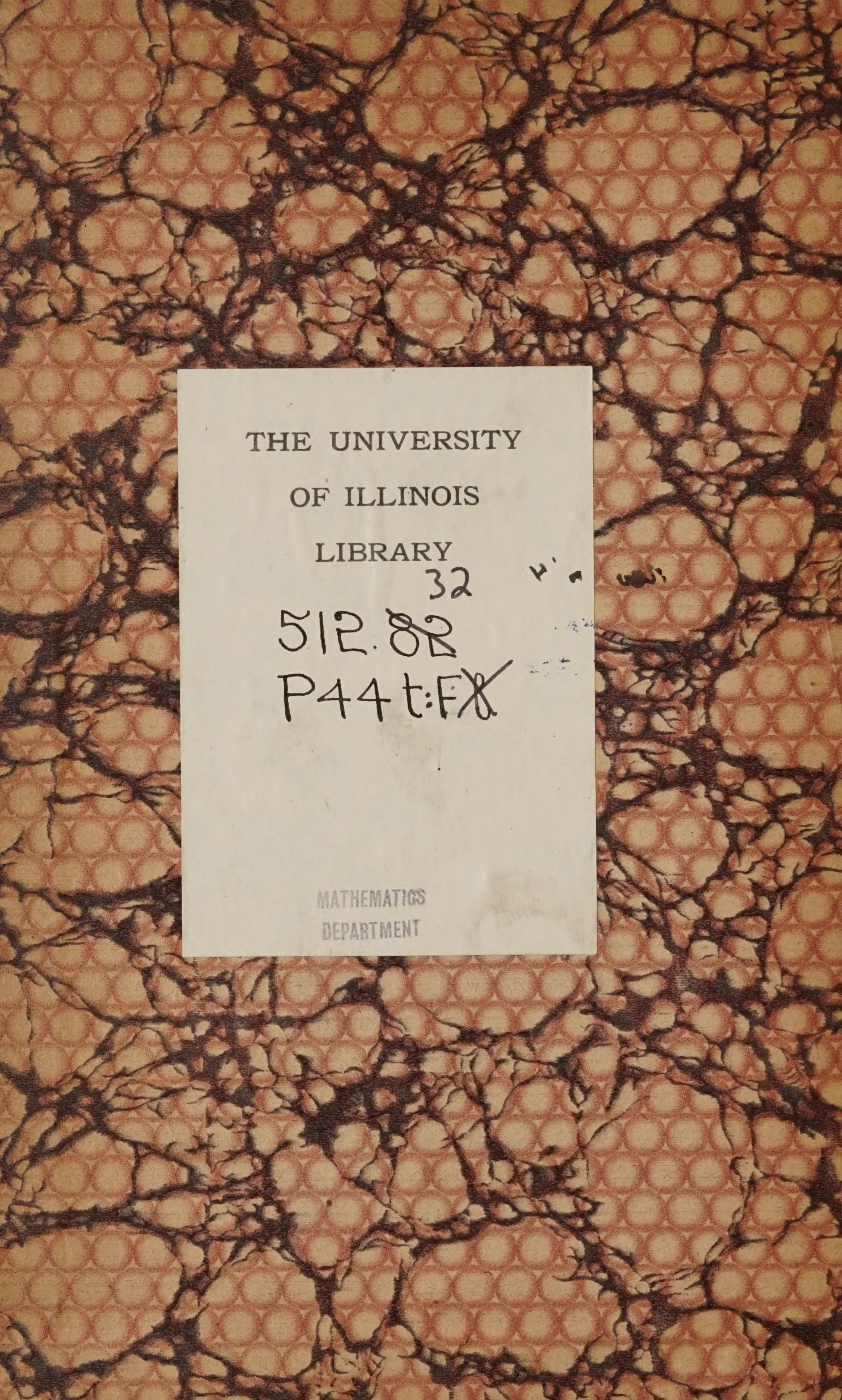
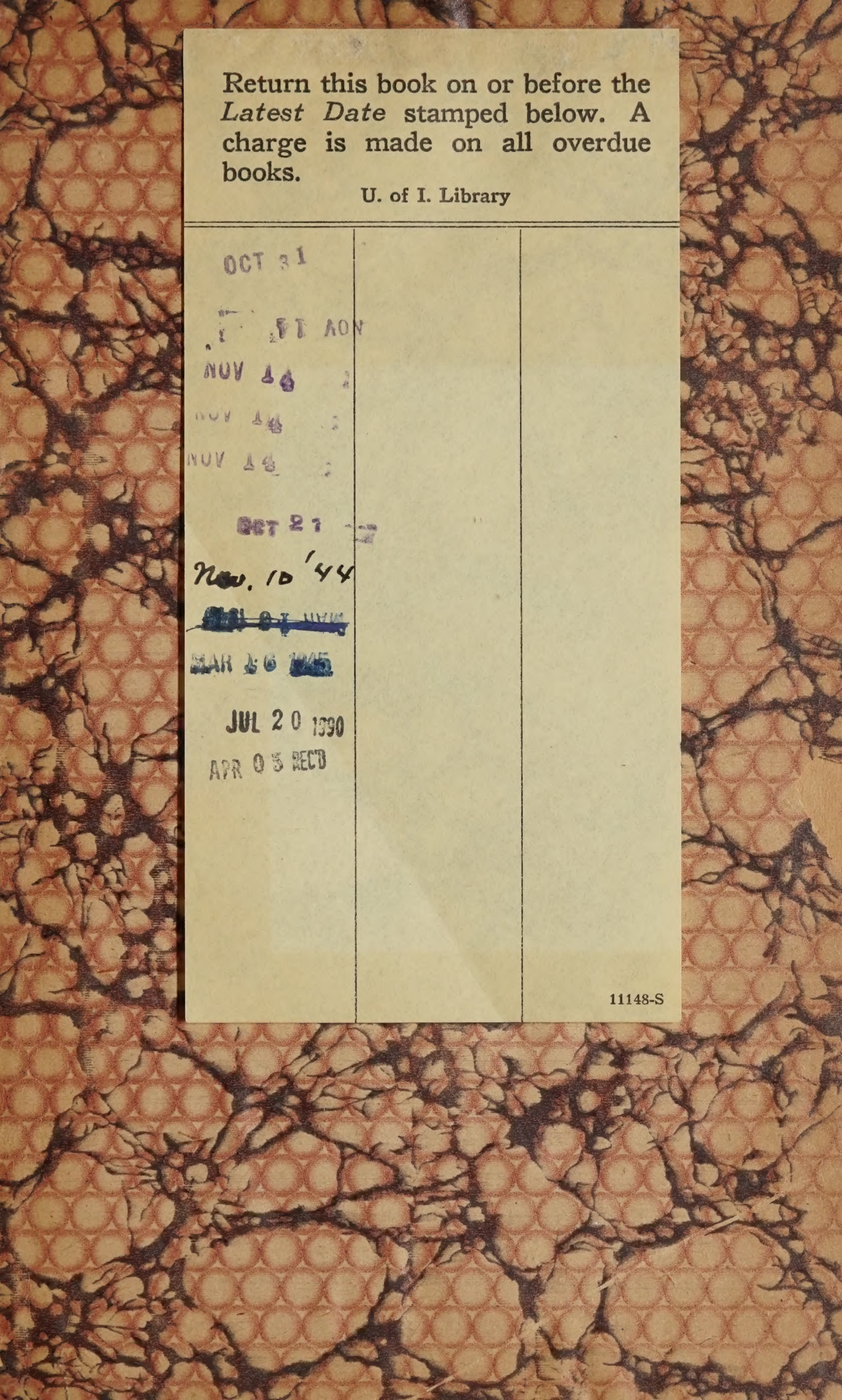








THÉORIE

DES

ÉQUATIONS ALGÉBRIQUES.

CHEZ LES MÊMES ÉDITEURS.

DU MÊME AUTEUR :

Méthodes et théories pour la résolution des problèmes de constructions géométriques, avec application à plus de 400 problèmes; traduit par O. Chemin.

Deuxième édition............. 4 fr.

THÉORIE

DES

ÉQUATIONS ALGÉBRIQUES

PAR

JULIUS PETERSEN,

PROFESSEUR À L'UNIVERSITÉ DE COPENHAGUE,

MEMBRE DE L'ACADÉMIE ROYALE DES SCIENCES.

TRADUCTION PAR

H. LAURENT,

Examinateur d'admission à l'École Polytechnique de Paris.



PARIS,

GAUTHIER-VILLARS ET FILS, IMPRIMEURS-LIBRAIRES

DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,

Quai des Grands-Augustins, 55.

—

1897

PRÉFACE DU TRADUCTEUR.

Je n'ai pas la prétention de faire l'éloge de la *Théorie des équations algébriques* de M. Petersen, ce Livre est connu et apprécié en France, et depuis longtemps on en désirait une traduction.

Sous un volume relativement petit, l'édition française que nous publions aujourd'hui contient les matières développées dans la plupart des Traités d'Algèbre supérieure, mais il contient, en outre, une théorie des équations résolubles au moyen d'équations du second degré avec la condition nécessaire et suffisante pour qu'un problème de Géométrie puisse être résolu au moyen de la règle et du compas; c'est, je crois, le seul Traité didactique dans lequel cette question importante se trouve traitée (¹). Il contient aussi une théorie entièrement nouvelle de la théorie des formes binaires (²), due

(¹) Le Chapitre relatif aux équations résolubles au moyen de racines carrées est tout à fait original; il est extrait de la thèse soutenue par M. Petersen pour obtenir le grade de docteur en 1871.

(²) Cette théorie des covariants a été donnée en 1879-1880.

à M. Petersen, qui n'existait pas dans l'édition originale et qui, bien entendu, n'a encore paru dans aucun Traité classique; cette théorie, qui fait l'objet du dernier Chapitre, sera lue avec intérêt, je l'espère, non seulement par les jeunes étudiants de nos Facultés et de nos Lycées, mais encore par leurs maîtres et par les savants.

Les personnes qui n'ont pas encore lu l'Ouvrage de M. Petersen et qui voudront bien étudier dans cette traduction, remarqueront la simplicité et la clarté de l'exposition qui font le charme de ce Traité d'Algèbre. Pour le lire avec fruit, il suffit de posséder les parties les plus élémentaires des Mathématiques, avec les quelques notions de Calcul différentiel enseignées dans les cours de nos Lycées qui préparent aux Écoles Polytechnique et Normale. Les candidats à ces Écoles trouveront, dans les trois premières Parties, le développement des matières exigées aux examens d'admission, avec de nombreuses applications. Ils y trouveront la démonstration de théorèmes utiles pour la délimitation et la séparation des racines, de nombreuses méthodes d'élimination, de curieuses méthodes d'approximation, peu connues en France, et cependant fort intéressantes.

Les élèves forts et qui ne travaillent pas dans le but exclusif d'entrer dans une École liront avec intérêt la théorie des équations abéliennes et le Chapitre re-

latif à l'équation du cinquième degré, où l'impossibilité de la résolution de cette équation se trouve établie par des moyens tout à fait élémentaires; et même, la théorie des équations résolubles au moyen d'équations du second degré, qui conduit à trouver les conditions nécessaires et suffisantes pour qu'un problème de Géométrie puisse être résolue au moyen de la règle et du compas.

La quatrième et la cinquième Partie contiennent : 1° la théorie des substitutions de lettres et des équations algébriques avec l'exposé des recherches d'Abel et de Galois; 2° la théorie des formes linéaires, dont nous avons parlé plus haut. Ces dernières Parties s'adressent plus particulièrement aux élèves de nos grandes Écoles; les maîtres même y trouveront l'occasion de s'instruire.

Je termine en remerciant M. Petersen d'avoir bien voulu me permettre de traduire son Traité d'Algèbre et de mettre mes compatriotes à même de profiter des excellentes choses qu'il contient.

H. LAURENT.

TABLE DES MATIÈRES.

PREMIÈRE PARTIE.

SUR DES ÉQUATIONS EN GÉNÉRAL.

CHAPITRE I.

Pages

Propriétés générales des équations algébriques I

Sur les expressions imaginaires. Fonctions rationnelles entières. Nombres des racines d'une équation. Racines conjuguées des équations à coefficients réels. Détermination de la racine commune à deux équations. Condition pour que deux équations aient des racines communes. Racines égales. Expressions des coefficients en fonction des racines.

CHAPITRE II.

Relations entre les coefficients et les racines.................. 26

Fonctions symétriques des racines. Formules de Newton. Autres fonctions symétriques. Nouvelle méthode pour le calcul des fonctions symétriques des racines. Formules générales pour le calcul de s_p et de a_p. Équation aux carrés des différences. Fonctions rationnelles des racines.

CHAPITRE III.

Sur l'élimination... 44

Élimination d'une quantité. Application de la théorie des fonctions symétriques. Méthode de Labatie. Méthode d'Euler. Méthode de Sylvester. Méthodes de Bézout et de Laurent. Systèmes de plusieurs équations à plus de deux inconnues. Théorème de Bézout. Théorème de Jacobi. Méthode de Poisson.

CHAPITRE IV.

Pages

Transformation des équations 72

Transformation linéaire. Équations réciproques. Formation des équations dans lesquelles une racine est fonction de plusieurs racines d'une équation donnée. Méthode de Tschirnaus pour faire disparaître des termes d'une équation.

DEUXIÈME PARTIE.

SUR LA SOLUTION ALGÉBRIQUE DES ÉQUATIONS.

CHAPITRE I.

L'équation du troisième degré ou l'équation cubique 89

Méthode de Hudde. Méthode de Lagrange. Méthodes de Tschirnaus et d'Euler.

CHAPITRE II.

L'équation du quatrième degré ou équation biquadratique 96

Méthode de Lagrange. Méthode de Descartes. Méthode de Ferrari. Méthodes de Tschirnaus et d'Euler. Étude approfondie de la Méthode de Descartes.

CHAPITRE III.

L'équation binome.. 103

Expression des racines au moyen des lignes trigonométriques. Propriétés des racines. Application de la théorie des équations réciproques aux équations binomes.

CHAPITRE IV.

L'équation du cinquième degré 112

Impossibilité de résoudre cette équation algébriquement.

CHAPITRE V.

Pages

Décomposition des polynomes rationnels en facteurs rationnels... 117

Facteurs du premier degré. Expression générale d'un facteur de $f(x)$.

CHAPITRE VI.

Équations abéliennes.. 124

Équations dans lesquelles une racine peut s'exprimer rationnellement en fonction d'une autre. Équation abélienne dont les racines forment un groupe. Examen du cas où le degré de l'équation n'est pas un nombre premier. Sur les équations irréductibles dont deux racines sont liées par la relation $x_1 x_2 + a x_1 + b x_2 + c = 0$. Résolution algébrique des équations binomes. Division de la circonférence en 17 parties égales. Réduction de l'équation $x^{13} = 1$. Propriété de l'équation $\frac{x^p - 1}{x - 1} = 0$ où p est premier.

CHAPITRE VII.

Équations résolubles à l'aide de racines carrées................. 150

Forme des racines. Résolution de l'équation. Condition pour qu'il soit possible de résoudre l'équation. Application à un problème de Géométrie. Intersection d'un faisceau avec une courbe du quatrième ordre.

TROISIÈME PARTIE.

SUR LA RÉSOLUTION NUMÉRIQUE DES ÉQUATIONS.

CHAPITRE I.

Séparation des racines.. 167

Limites des racines réelles. Nombre des racines comprises entre deux nombres donnés. Théorème de Descartes. Théorème de Budan. Théorème de Rolle. Théorème de Sturm. Application du théorème de Sturm aux racines imaginaires. Séparation des racines réelles. Méthode de Fourier. Théorème de Newton. Généralisation du théorème de Descartes.

CHAPITRE II.

Pages

Calcul des racines des équations numériques.................. 203

Calcul des racines commensurables. Interpolation. Méthode d'approximation de Newton. Méthode de Lagrange. Méthode de Horner. Calcul des racines imaginaires.

QUATRIÈME PARTIE.

SUR LES SUBSTITUTIONS.

CHAPITRE I.

Des substitutions en général.............................. 231

Ordre des substitutions. Substitutions circulaires. Substitutions semblables et échangeables. Substitutions positives et négatives.

CHAPITRE II.

Substitutions conjuguées ou groupes........................ 245

Théorème de Lagrange. Substitutions permutables avec un groupe. Sur la formation de quelques groupes. Le groupe alterné. Groupes que l'on peut former par la multiplication des substitutions d'autres groupes. Théorème de Cauchy. Groupes transitifs et intransitifs. Sur les groupes transitifs qui contiennent d'autres groupes également transitifs. Groupe d'une fonction et nombre des valeurs qu'elle peut acquérir. Indice d'un groupe. Des substitutions linéaires.

CHAPITRE III.

Théorie de Galois...................................... 276

Groupe d'une équation. Propriétés du groupe d'une équation. Réduction du groupe au moyen de quantités adjointes. Adjonction des racines d'une équation auxiliaire.

CHAPITRE IV.

Pages

Applications de la théorie de Galois 292

Équations abéliennes. Équation de Galois. Équations dont le groupe a pour ordre une puissance d'un nombre premier. Équation de Hesse. Groupe de monodromie d'une équation.

CINQUIÈME PARTIE.

SUR LES FORMES.

CHAPITRE I.

Covariants des formes binaires 311

Formes et substitutions linéaires. Symboles. Coefficients et fonctions transformées. Semi-invariants. Covariants. Formation de nouveaux semi-invariants. Systèmes généraux de formes jusqu'à $n = 4$. Formes quadratiques à plusieurs variables. Substitutions orthogonales. Invariants.

NOTE.

Sur l'équation $x^n = 1$ 346

ERRATA.

Pages	Lignes	Au lieu de	Lire
15	6	$2n$	n.
23	7 en rem.	$p-1$ fois appartient à ligne 9.	
38	formule (9)	s_p	s_n.
45	13 en rem.	Ainsi,	Mais.
52	2	α	d.
54	17	y^3	y^2.
59	15 en rem.	(1)	(2).
60	8	en	m.
62	12 en rem.	b^2x	b^2z.
67	8	$x^{\mu-1}, y^{\mu-1}, z^{\mu-1}$	$x^{\mu-1}y^{\mu-1}z^{\mu-1}$
77	7	$6x+4$	$6x-4$.
84	14	Terrard	Jerrard.
84	3 en rem.	d'eux	des restants.
89	6	irréductible.	réductible.
91	2	x^2	x^3.
101	11 en rem.	$\alpha_2+\alpha_3$	$\alpha_2-\alpha_3$.
105	6 en rem.	racines	racines imaginaires.
106	13	qui sont... binomes appartient à ligne 15 après celles	
111	6	divisibles.	divisible.
120	6 en rem.	2	4.
122	14 en rem.	on peut	on le peut.
122	13 en rem.	un	en un.
130	2 en rem.	ω	$\frac{2\pi}{n}$.
140	1 en rem.	$+-$	$=+$.
141	3 en rem.	p	car p.
152	5 et 6	c	c_1
153	2 en rem.	n	p.
160	6 en rem.	et	où.
179	7 en rem.	$-q$	$\mp q$.
187	10 en rem.	$+\infty$	$-\infty$.
217	1 en rem.	32	3.
221	17	3490	34940
235	5 en rem.	*cabd*	*bdea*.

Pages	Lignes	Au lieu de	Lire
243	3 en rem.	des trois	trois des.
248	4 en rem.	...	N^{-1}.
		N^{-1}	....
250	10	$(be), (cd)$	$(be)(cd)$.
251	11 en rem.	ces	les.
253	6 en rem.	un	un plus
256	2 en rem.	a,	,.
269	5	γ	γ_1
278	4 en rem.	A'	A_r
285	1	$z = z$	$z = z_i$
288	11	pour	par
290	14	un	le
292	1 en rem.	fonctions	équations
299	9	Q	G
303	11 en rem.	β_1	β
304	11	lignes triples	lignes
»	»	ligne triple	ligne d'un triple
»	12	lignes triples	triples de lignes
»	19	pour la fonction	par l'adjonction
	10 en rem.	Q_1	G_1
313	14 en rem.	fonctions	formes
318	1 en rem.	$x_0^{\mu} + \ldots$	x_0^{p}
319	11 en rem.	p	μ.

THÉORIE

DES

ÉQUATIONS ALGÉBRIQUES.

CHAPITRE I.

PROPRIÉTÉS GÉNÉRALES DES ÉQUATIONS ALGÉBRIQUES.

Sur les expressions imaginaires.

1. Si l'on désigne par i l'expression imaginaire $\sqrt{-1}$, la forme générale d'une quantité imaginaire ou d'un nombre complexe sera

$$a + bi,$$

où a et b sont réels. Si l'on pose

(1) $$a = r\cos\theta, \qquad b = r\sin\theta,$$

on aura

(2) $$a + bi = r(\cos\theta + i\sin\theta)$$

et

(3) $$r = \sqrt{a^2 + b^2}, \qquad \operatorname{tang}\theta = \frac{b}{a}\cdot$$

r est le module, il est essentiellement positif; θ est l'argument, (3) donne pour θ deux valeurs, mais (1) montre que $\cos\theta$ a le signe de a et $\sin\theta$ celui de b, et, comme ces signes déterminent le quadrant où se termine θ, l'arc compris entre 0 et 2π, dont la tangente est $\operatorname{tang}\theta$, se trouve bien déter-

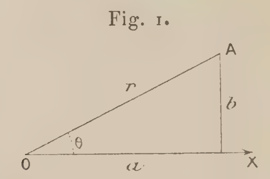
miné. En réalité, θ possède une infinité de valeurs positives ou négatives différant entre elles de $2p\pi$, où p désigne un entier arbitraire positif ou négatif. Dans la suite, il sera sous-entendu que l'on peut toujours ajouter à l'argument ce nombre $2p\pi$. On représente encore, pour abréger, la quantité qui a pour module r et pour argument θ par la notation r_θ.

Exemples :

$$-1 = 1_\pi, \qquad i = 1_{\frac{\pi}{2}}, \qquad -1 + i\sqrt{3} = 2_{\frac{2\pi}{3}}, \qquad -1 - i\sqrt{3} = 2_{\frac{4\pi}{3}}.$$

2. L'imaginaire $a + bi$ peut être représentée par un point. Soient O (*fig.* 1) une origine et OX un axe orienté ; un point A

Fig. 1.



est déterminé quand on donne le rayon vecteur r et l'angle θ qu'il fait avec l'axe OX ; on peut représenter ce point par la notation r_θ ; on voit que les quantités réelles sont représentées par les points de l'axe OX. On voit aussi que r représente en quelque sorte la valeur numérique de r_θ, et que le facteur $\cos\theta + i\sin\theta$ en détermine la direction, il joue le rôle d'un signe directif. Les signes + et — désignent deux directions opposées sur l'axe OX, de même i et $-i$ représentent les deux directions opposées perpendiculaires à OX. Nous allons montrer comment, en généralisant la notion d'addition, on peut déduire de ces directions toutes les autres.

Au lieu de dire que l'imaginaire r_θ représente le point A, on peut dire que le rayon orienté OA est représenté par r_θ.

Les deux imaginaires $a + bi$, $a - bi$ sont dites *conjuguées ;* elles ont même module, leurs arguments sont égaux et de signes contraires, les points qu'elles représentent sont symétriques par rapport à l'axe OX.

3. *Calcul des imaginaires.* — Nous allons maintenant généraliser la notion d'addition, de manière à obtenir pour les imaginaires un calcul analogue à celui des quantités réelles. Soit donnée la formule

$$(a+bi)+(a_1+b_1i)=a+a_1+(b+b_1)i;$$

les points qui représentent les parties de la somme ont respectivement pour coordonnées a, b et a_1, b_1, celui qui représente la somme, a pour coordonnées $a+a_1$ et $b+b_1$. Ces trois points et l'origine des coordonnées sont les sommets d'un parallélogramme dont les côtés sont r et r_1, les directions de ces côtés sont déterminées par les angles θ et θ_1. *L'addition se ramène donc à la recherche de la résultante de deux droites ayant pour longueurs les modules et pour directions les arguments des quantités à ajouter*, et l'on voit l'interprétation géométrique de ce fait qu'une somme ne change pas quand on intervertit l'ordre de ses parties.

Lorsque la somme de plusieurs imaginaires est nulle, après avoir composé les droites qui représentent les parties, on revient à l'origine et la figure se réduit à un polygone fermé : on peut donc dire que la somme des côtés d'un polygone fermé est nulle, si l'on sous-entend que chaque côté représente une imaginaire, et qu'il est déterminé en grandeur et en direction, ce qui détermine le sens dans lequel le polygone doit être parcouru. On peut dire aussi que le point final représente la même imaginaire quel que soit le chemin parcouru. Ainsi la formule (2) montre que l'on arrive au même point, soit en parcourant le rayon r dans la direction θ, soit en parcourant a dans la direction $+1$ et b dans la direction i. Il résulte des considérations précédentes que *le module d'une somme est moindre que la somme des modules de ses parties,* pourvu que les parties n'aient pas toutes le même argument. Dans ce dernier cas, en effet, le module de la somme serait égal à la somme des modules de ces parties.

La *soustraction* revient à une addition avec changement de signe de la partie à soustraire.

La notion de *multiplication* résulte de la considération de la formule

$$r(\cos\theta + i\sin\theta)\, r_1(\cos\theta_1 + i\sin\theta_1)$$
$$= r.r_1[\cos(\theta + \theta_1) + i\sin(\theta + \theta_1)]$$

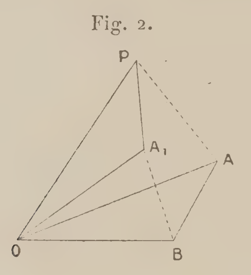
ou

$$(4) \qquad r_\theta\, r_{1\theta_1} = (rr_1)_{\theta+\theta_1}.$$

On voit que *le module d'un produit est égal au produit des modules de ses facteurs, et que son argument est égal à la somme des arguments des facteurs.*

La multiplication par un facteur revient ainsi à une multiplication par le module de ce facteur (dans le sens ordinaire du mot *multiplication*), suivie d'une *rotation* égale à l'argument de ce facteur. Soient A et A_1 (*fig.* 2) les points qui re-

Fig. 2.



présentent les facteurs, B le point qui représente l'unité $+1$, et P celui qui représente le produit; on voit facilement que le triangle OBA est semblable à OA_1P.

Ainsi le triangle, formé par l'unité et l'un des facteurs, est semblable au triangle formé par l'autre facteur et le produit. *Le produit est formé avec le multiplicande comme le multiplicateur est formé avec l'unité.*

L'échange des points A et A_1 fournirait encore des triangles semblables; c'est l'interprétation géométrique du théorème relatif à la possibilité de l'interversion des facteurs.

Exemple :

$$(-1)(-2) = 1_\pi . 2_\pi = 2_{2\pi} = 2, \qquad i^2 = 1_{\frac{\pi}{2}} 1_{\frac{\pi}{2}} = 1_\pi = -1.$$

La *division* se ramène à la multiplication. Quant à l'*élévation aux puissances* et à l'*extraction des racines*, elles donnent lieu aux formules (n étant un entier positif)

$$(5)\qquad \begin{cases} (r_\theta)^n = r^n_{n\theta}, \\ \sqrt[n]{r_\theta} \;\; = (\sqrt[n]{r})_{\frac{\theta}{n}}. \end{cases}$$

Dans le second membre de la dernière formule, on doit supposer à θ des valeurs de la forme $\theta + 2p\pi$, et des valeurs différentes de p pourront fournir des solutions différentes.

Dans la suite, on fera usage d'exposants fractionnaires, lorsqu'on suppose toutes ses valeurs à une racine, au contraire, on fera usage du signe radical, lorsque l'on voudra représenter une valeur bien déterminée; ainsi on aura

$$(6)\qquad (r_\theta)^{\frac{1}{n}} = (\sqrt[n]{r})_{\frac{2p\pi+\theta}{n}},$$

où p doit recevoir les valeurs $0, 1, 2, \ldots, (n-1)$. $p=n$ donne le même résultat que $p=0$; $p=n+\alpha$ donne le même résultat que $p=\alpha$. Ainsi le nombre des valeurs réellement distinctes de (6) est n; et, comme leurs directions partagent l'espace en n parties égales déterminées par les directions

$$\frac{\theta}{n}, \quad \frac{\theta}{n} + \frac{2\pi}{n}, \quad \ldots, \quad \frac{\theta}{n} + (n-1)\frac{2\pi}{n},$$

$(r_\theta)^{\frac{1}{n}}$ aura au plus deux valeurs réelles données par les formules

$$\frac{2p\pi+\theta}{n} = 0 \qquad \text{ou} \qquad \frac{2p\pi+\theta}{n} = \pi.$$

Dans le premier cas, on a $\theta = 0$, $p = 0$; dans le second cas, on a $\theta = 0$ et $2p = n$ ou $\theta = \pi$ et $2p+1 = n$. Si r_θ est imaginaire, ses racines sont imaginaires; s'il est positif, une racine sera positive, l'autre négative si n est pair; une seule racine sera positive, si n est impair.

Enfin, si r_θ est négatif, une racine sera négative si n est impair, et toutes les racines seront imaginaires si n est pair.

En combinant les résultats précédents, on obtient des théorèmes analogues au sujet des exposants négatifs et fractionnaires

$$(r_\theta)^{-n} = \frac{1}{(r_\theta)^n} = \frac{1}{r^n_{n\theta}} = (r^{-n})_{-n\theta},$$

$$(r_\theta)^{\frac{s}{q}} = \left[(r_\theta)^{\frac{1}{q}}\right]^s = (\sqrt[q]{r^s})_{\frac{s}{q}(\theta+2p\pi)}.$$

Si la fraction $\frac{s}{q}$ peut être réduite à une plus simple expression, l'expression de $(r_\theta)^{\frac{s}{q}}$ peut se simplifier également.

Exemple I :

$$\left(\frac{-1+i\sqrt{3}}{2}\right)^{\frac{1}{3}}, \qquad r = 1, \qquad \theta = \frac{2}{3}\pi;$$

les trois valeurs de cette expression sont

$$\cos 40° + i \sin 40°, \qquad \cos 160° + i \sin 160°, \qquad \cos 280° + i \sin 280°.$$

Exemple II :

$$(-8)^{\frac{1}{3}}, \qquad r = 8, \qquad \sqrt[3]{r} = 2, \qquad \theta = \pi;$$

les valeurs de $(-8)^{\frac{1}{3}}$ sont

$$2_{\frac{\pi}{3}}, \quad 2_\pi \quad \text{et} \quad 2_{\frac{5\pi}{3}} \quad \text{ou} \quad 1+i\sqrt{3}, \quad -2 \quad \text{et} \quad 1-i\sqrt{3}.$$

Nous allons maintenant appliquer la théorie précédente à des considérations géométriques.

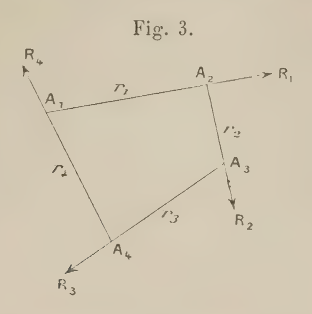
On sait que l'expression

$$\frac{x_2-x_1}{x_3-x_2} : \frac{x_1-x_4}{x_4-x_3}$$

reste invariable quand on remplace x_1, x_2, x_3, x_4 par $\frac{1}{x_1}$, $\frac{1}{x_2}$, $\frac{1}{x_3}$, $\frac{1}{x_4}$. Supposons les quantités x imaginaires et représentées par les points A_1, A_2, A_3, A_4 (*fig.* 3). Alors x_2-x_1 sera représenté en grandeur et en direction par A_1A_2. Si l'on parcourt les seg-

ments analogues dans l'ordre A_1, A_2, A_3, A_4; si l'on désigne leurs modules par r_1, r_2, r_3, r_4, et leurs directions par de

Fig. 3.



grandes lettres, X désignant la direction des quantités positives, on aura

$$x_2 - x_1 = r_{1(XR_1)}, \quad \ldots.$$

Le rapport considéré devient alors

$$\frac{r_1(XR_1)}{r_2(XR_2)} : \frac{r_4(XR_4)}{r_3(XR_3)};$$

il a pour module

$$\frac{r_1 r_3}{r_2 r_4}$$

et pour argument

$$(XR_1) + (R_2X) + (R_4X) + (XR_3) = (R_2R_1) + (R_4R_3).$$

Ainsi le module de notre expression est le rapport des produits des côtés opposés du quadrilatère $A_1A_2A_3A_4$, et l'argument de cette expression est la somme des angles opposés (et extérieurs); ces grandeurs restent inaltérées après la transformation, qui consiste à remplacer x par $\frac{1}{x}$ ou r_θ par $\left(\frac{1}{r}\right)_{-\theta}$; si $-\theta$ se change en θ, le point correspondant se change en son symétrique par rapport à l'axe des quantités positives; cela revient à changer la direction dans laquelle on compte les angles positifs; on obtient alors $\left(\frac{1}{r}\right)_\theta$. Notre proposition

a donc encore lieu si l'on remplace r_0 par $\left(\frac{1}{r}\right)_0$, et si nous changeons $-\theta$ en θ, de telle sorte que le produit des distances des deux points correspondant à l'origine soit égal à un. Les deux points en question sont alors *transformés l'un de l'autre par rayons vecteurs réciproques*. Nous venons donc de démontrer par l'Algèbre que, par une transformation par rayons vecteurs réciproques des sommets d'un quadrilatère, on n'altère pas le rapport des produits des côtés opposés pendant que la somme des angles opposés change son signe. Il est d'ailleurs indifférent que le quadrilatère soit concave ou convexe.

Fonctions rationnelles entières.

4. Étant donnée la fonction entière

$$f(z) = A_0 z^m + A_1 z^{m-1} + \ldots + A_{m-1} z, \tag{1}$$

on peut toujours choisir le module r de z assez petit pour que le module de $f(z)$ devienne et reste plus petit qu'une quantité donnée R.

En effet, soit a le plus grand module des coefficients de $f(z)$, on aura

$$\bmod f(z) < a(r^m + r^{m-1} + \ldots + r) \quad \text{ou} \quad < a\,\frac{r - r^{m+1}}{1 - r},$$

et si $r < 1$

$$\bmod f(z) < \frac{ar}{1 - r},$$

et $f(z)$ aura un module inférieur à R, si l'on prend

$$r < \frac{R}{a + R}.$$

Il résulte de là que, dans la fonction

$$z^n + P,$$

où P désigne une fonction entière dans laquelle les exposants de z sont supérieurs à n, on peut choisir le module de z assez petit pour que $\bmod \frac{P}{z^n}$ puisse être rendu plus petit

qu'une quantité donnée; si l'on change z en $\frac{1}{z}$, on voit, par suite, que l'on peut prendre le module de z assez grand pour que

$$\operatorname{mod} \frac{z^n}{P}$$

puisse surpasser toute quantité donnée, P désignant un polynome dans lequel tous les exposants de z sont inférieurs à n.

5. *Une fonction entière et rationnelle de z est continue* [1].

$f(z)$ est continue si, z étant quelconque, on peut prendre $\operatorname{mod} h$, tel que pour toutes les valeurs de h du module moindre ou égal, le module de la différence

$$f(z+h)-f(z)$$

devienne moindre qu'une quantité donnée si petite que l'on veut.

Cette différence, développée par la formule de Taylor, donne

$$f'(z)h+f''(z)\frac{h^2}{1.2}+\ldots+f^m(z)\frac{h^m}{1.2\ldots m},$$

et cette expression, comme on vient de le voir, peut être rendue aussi petite que l'on veut en choisissant $\operatorname{mod} h$ convenablement.

Il résulte de là que, si $f(z)$ est à coefficients réels, et si cette fonction prend des valeurs de signes contraires pour deux valeurs de z, elle doit s'annuler pour une certaine valeur de z comprise entre celles-ci.

6. *Une fonction entière réelle de deux variables réelles x et y ne peut changer de signe quand x et y varient d'une manière continue sans passer par zéro.*

Dans le cas contraire, la fonction en un certain point devrait passer brusquement d'une valeur positive à une valeur

---

[1] Cela résulte aussi de ce qu'une pareille fonction a une dérivée bien déterminée pour chaque valeur de la variable.

négative ou inversement, de telle sorte que

$$f(x+h, y+k) - f(x, y)$$

ne pourrait pas devenir moindre qu'une quantité donnée pour des valeurs suffisamment petites de h et k; cela est impossible, car cette différence peut s'écrire

$$f(x+h, y+k) - f(x+h, y) + f(x+h, y) - f(x, y),$$

et il résulte de ce que nous avons dit plus haut que chacune des deux différences dont se compose l'expression précédente peut être rendue aussi petite que l'on veut, la première en prenant k, la seconde en prenant h suffisamment petit.

La courbe dont l'équation est

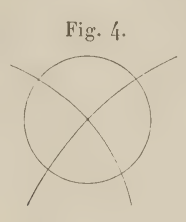
$$f(x, y) = 0$$

partage le plan en régions finies ou infinies; si l'on considère deux points, si l'on substitue les valeurs de leurs coordonnées dans $f(x, y)$, et si l'on obtient des résultats de signes contraires, on ne pourra passer d'une manière continue de l'un à l'autre sans traverser la courbe. Les régions du plan seront regardées comme positives ou négatives par rapport à la courbe, suivant que les coordonnées des points de ces régions substitués à la place de x et y rendront $f(x, y)$ positif ou négatif. Pour passer d'une région positive à une région négative, il faut traverser la courbe un nombre impair de fois; pour passer d'une région positive à une région positive, il faut la traverser un nombre pair de fois. Si l'on traverse un point où se coupent deux branches de courbe, il faut compter le passage par un tel point comme un double passage.

Comme on peut supposer $f(x, y)$ écrit avec un signe quelconque, le signe d'une région est arbitraire, mais on peut convenir d'écrire $f(x, y)$ de telle sorte que le terme qui ne contient ni x ni y soit positif. De cette façon, l'origine sera dans la région positive et les signes des autres régions seront déterminés.

7. Si l'on considère deux courbes $A = 0$ et $B = 0$, leur ensemble partagera le plan en régions où le produit AB sera ou positif ou négatif, suivant que A et B y auront le même signe ou des signes contraires. Considérons un point d'intersection des deux courbes (*fig.* 4), et décrivons autour de ce

Fig. 4.

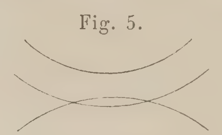


point une petite courbe fermée; son périmètre sera partagé par les branches des courbes $A = 0$, $B = 0$ en quatre parties. Parcourons la petite courbe et déterminons en chacun de ses points la valeur de AB; toutes les fois que AB s'annule, son signe change et l'on franchit une branche du nœud. Appelons les portions de la petite courbe, parties positives ou négatives suivant que sur ces parties AB est positif ou négatif; deux parties opposées seront positives, les deux autres seront négatives; chaque fois que l'on traverse une branche du nœud, on passe d'une partie positive à une partie négative ou inversement. Si l'on effectue le parcours dans un sens déterminé, on rencontre deux espèces de points d'intersection : ceux où, en traversant la courbe A, on passe du positif au négatif; ceux où, en traversant la courbe A, on passe du négatif au positif. On trouve un exemple de ces points dans l'intersection de deux cercles.

Si, pour chaque point d'intersection des courbes A et B, on fait la différence du nombre de fois où, dans un parcours autour de ces points dans le sens positif, on traverse la courbe A en passant du positif au négatif, et où on la traverse en passant du négatif au positif, on trouve $+2$ pour certains points et -2 pour d'autres, les uns seront appelés de *première espèce,* les autres seront de *seconde espèce.* Si l'on ajoute toutes ces différences, on obtient un nombre qui est le double de la

différence Δ entre les nombres de points de la première et de la seconde espèce. Ce nombre est celui que l'on trouverait si l'on parcourait une courbe fermée renfermant, dans son intérieur, tous les points d'intersection des courbes A et B. En effet, en déformant une pareille courbe, l'ordre dans lequel elle rencontre A et B ne peut se modifier qu'en passant par un point d'intersection de A et B, et en quittant un point où elle touche A ou B. Elle gagne où elle perd alors deux points d'intersection avec ces courbes (*fig.* 5). Ces derniers points n'ont

Fig. 5.

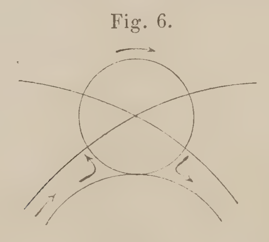


pas d'influence sur la valeur de la différence considérée, car ils se suivent immédiatement; si ce sont des intersections avec B, ils ne comptent pas; si ce sont des intersections avec A, ils ne changent pas la différence, parce que, une fois, on passe du négatif au positif, et une autre fois du positif au négatif.

Puisque deux semblables points, pris simultanément, n'ont pas d'influence sur les autres points d'intersection, ils ne peuvent modifier la différence Δ dont nous nous occupons. Celle-ci ne peut donc changer que quand on passe par un point d'intersection de A et B.

Considérons une petite courbe fermée (*fig.* 6), ne coupant

Fig. 6.



ni A et B, et pour laquelle la différence Δ est nulle; agrandissons cette courbe jusqu'à ce qu'elle touche une des petites

courbes décrites autour d'un point d'intersection de A et B, et, à ce moment, adjoignons-lui cette petite courbe; la différence croîtra de $+2$ ou -2, suivant que l'intersection sera de première ou de seconde espèce; on peut donc énoncer le théorème suivant :

Étant données deux courbes A, B, *si l'on parcourt une courbe fermée dans un sens déterminé, la différence du nombre des points de première et de seconde espèce contenus à l'intérieur de cette courbe est la moitié de la différence du nombre de fois que l'on passe du positif au négatif et du nombre de fois que l'on passe du négatif au positif, en traversant la courbe* A.

S'il n'y a que des points d'une seule espèce, on peut déterminer ainsi le nombre des points réels d'intersection des courbes A et B contenus dans un contour fermé. Le théorème, du reste, est vrai quelque rapprochés que soient les points d'intersection, et, si plusieurs sont confondus, il a encore lieu en comptant chaque point autant de fois qu'il renferme d'intersections confondues.

Nombre des racines d'une équation.

8. Considérons une équation du degré n

$$(1) \qquad f(z) = A_0 z^n + A_1 z^{n-1} + \ldots + A_n = 0,$$

à coefficients réels ou imaginaires; posons

$$z = x + yi,$$

x et y désignant des nombres réels; en séparant les parties réelles et imaginaires, on a

$$(2) \qquad f(x+yi) = A + Bi,$$

A et B désignant des fonctions réelles de x et y; la condition nécessaire et suffisante pour que $x + yi$ soit racine de l'équa-

tion (1) est que l'on ait

$$(3) \qquad A = 0, \qquad B = 0;$$

les racines seront donc représentées par les points d'intersection réels des courbes A et B : nous les appellerons *points racines* [1].

Maintenant appliquons à ces courbes le théorème démontré tout à l'heure. A cet effet, décrivons un cercle assez grand pour contenir toutes les intersections des courbes A et B, si elles se coupent; divisons l'équation (1) par A_0, elle prendra la forme

$$(4) \qquad z^n + a_\nu z^{n-1} + \ldots = 0,$$

et, en posant $z = x + yi = r(\cos\theta + i\sin\theta)$,

$$(5) \qquad A = r^n \cos n\theta + ar^{n-1}\cos[(n-1)\theta + \nu] + \ldots = 0,$$

$$(6) \qquad B = r^n \sin n\theta + ar^{n-1}\sin[(n-1)\theta + \nu] + \ldots = 0,$$

on peut prendre le rayon r du cercle assez grand, pour que les premiers termes de (5) et (6) donnent, avec une approximation aussi grande que l'on veut, les points d'intersection des courbes avec le cercle; on a alors

$$\cos n\theta = 0, \qquad \sin n\theta = 0,$$

d'où

$$\theta = \frac{(2p+1)\pi}{2n}, \qquad \theta = \frac{p\pi}{n}.$$

---

[1] Les courbes A et B ne sont pas quelconques, elles dépendent l'une de l'autre; on a en effet, en différentiant,

$$f'(x+yi) = \frac{\partial A}{\partial x} + \frac{\partial B}{\partial x} i,$$

$$i f'(x+yi) = \frac{\partial A}{\partial y} + \frac{\partial B}{\partial y} i,$$

d'où l'on tire

$$\frac{\partial B}{\partial x} = -\frac{\partial A}{\partial y}, \qquad \frac{\partial A}{\partial x} = \frac{\partial B}{\partial y}.$$

Les points d'intersection avec le cercle des courbes A et B, à mesure que le rayon du cercle croît, tendent donc à partager la circonférence en $4n$ parties égales, et ces points se suivent alternativement; la différence Δ, considérée plus haut, du nombre des points de première et de seconde espèce est donc $2n$, il y a donc au moins n points d'intersection contenus dans le cercle. Donc

Une équation de degré n a au moins n racines.

9. *Si α_1 est une racine de $f(z) = 0$, le polynome $f(z)$ est divisible par $z - \alpha_1$.*

En effet, on peut poser

$$f(z) = (z - \alpha_1)Q + R,$$

Q désignant une fonction entière, et R un nombre indépendant de z. Cette identité doit avoir lieu pour $z = \alpha_1$, et l'on a

$$R = 0;$$

car R ne contient pas z, et il ne change pas en remplaçant z par α_1.

Soit α_2 une autre racine de l'équation, elle doit annuler $(z - \alpha_1)Q$ et par suite Q, donc

$$Q = (z - \alpha_2)Q_1,$$

donc

$$f(z) = (z - \alpha_1)(z - \alpha_2)Q_1,$$

et ainsi de suite.

Inversement, on voit facilement que α est racine de $f(z) = 0$ quand $(z - \alpha)$ divise $f(z)$. A chaque racine de $f(z)$ correspond donc un facteur de $f(z)$ de la forme $z - \alpha$, et réciproquement. Comme un polynome du degré n ne peut avoir plus de n facteurs du premier degré, une équation de degré n ne saurait avoir plus de n racines. *En combinant ce résultat*

avec le n° 8, on voit qu'une équation de degré n a n racines [1].

Si l'on appelle $\alpha_1, \alpha_2, \ldots, \alpha_n$ ces racines, on a

$$(7) \qquad f(z) = A_0(z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_n),$$

où A_0 est le coefficient de z^n dans $f(z)$.

10. On a supposé, dans la démonstration du théorème précédent, que les points d'intersection de A et B étaient simples, c'est-à-dire tels qu'une petite courbe tracée autour de chacun d'eux ne rencontrait chacune des courbes A, B que deux fois seulement. Si cela n'avait pas lieu, on ne trouverait n racines qu'en comptant chaque semblable point pour autant de fois qu'il y a de doubles passages du signe $+$ au signe $-$. Nous allons revenir sur ce cas.

Prenons pour origine un point racine $z = \alpha$; $z = 0$ doit satisfaire à l'équation, elle a donc la forme

$$(8) \qquad a_{\upsilon} z + b_{\upsilon_1} z^2 + \ldots = 0,$$

et l'on a

$$(9) \qquad A = ar\cos(\theta+\upsilon) + br^2\cos(2\theta+\upsilon_1) + \ldots = 0,$$

$$(10) \qquad B = ar\sin(\theta+\upsilon) + br^2\sin(2\theta+\upsilon_1) + \ldots = 0;$$

---

(1) On voit que les points racines doivent être des points de même espèce, de sorte que le théorème énoncé plus haut peut servir à déterminer le nombre des racines contenues dans un contour donné (théorème de Cauchy); on peut montrer que les deux espèces de points d'intersection pour les courbes A et B sont tels qu'il faut traverser la courbe

$$\frac{\partial A}{\partial x}\frac{\partial B}{\partial y} - \frac{\partial A}{\partial y}\frac{\partial B}{\partial x} = 0,$$

un nombre impair de fois pour aller d'un point d'une espèce à un point de l'autre espèce. Cette courbe n'a pas de branche réelle, car à l'aide des équations de la note de la page 14, le premier membre de son équation se change en une somme de deux carrés.

pour une petite valeur de r, on n'a besoin de considérer que les premiers termes. Tant que a n'est pas nul, chacune des courbes A et B ne coupe le petit cercle de rayon r qu'en deux points déterminés par les équations

$$\cos(\theta + \upsilon) = 0, \qquad \sin(\theta + \upsilon) = 0,$$

et l'on a affaire à un point d'intersection ordinaire. Si, au contraire, $a = 0$, les points d'intersection du cercle avec A et B seront donnés par

$$\cos(2\theta + \upsilon_1) = 0 \quad \text{et} \quad \sin(2\theta + \upsilon_1) = 0,$$

d'où il suit que chaque courbe possède en ce point un point double, et le petit cercle les coupe en 8 points, chaque équation donnant 4 valeurs pour θ. Un pareil point augmente la différence Δ de ± 4 et compte pour deux points racines. En général, un point devra compter pour p points si l'équation a pour premier terme un terme en z^p ou quand son premier membre est divisible par z^p; dans ce cas $f(z)$ est divisible par $(z - \alpha)^p$ et le *théorème que nous avons démontré n'est vrai que si, $f(z)$ étant divisible par $(z - \alpha)^p$, on compte la racine α comme équivalant à p racines.* On dit alors que l'équation a p racines égales à α, ou que α est une racine multiple d'ordre p.

11. *Deuxième démonstration de ce théorème que toute équation de degré n a n racines* (démonstration d'Argand, aussi appelée *démonstration de Cauchy*).

Il suffit de démontrer que toute équation a une racine, car on peut écarter cette racine par la division du premier membre de l'équation par un facteur du premier degré, on a alors une équation de degré moindre qui admet une racine, et ainsi de suite jusqu'à ce que l'on arrive à une équation du premier degré qui a une seule racine; on a ainsi déterminé successivement n racines dans le cas où l'équation est de degré n.

Pour établir que l'équation

$$f(z) = 0$$

a au moins une racine, nous chercherons à la vérifier pour une valeur

$$z_0 = r_\theta.$$

Si z_0 satisfait à l'équation, ce sera une racine, sinon $f(z)$ prendra pour $z = z_0$ une valeur Z_0 de module R; mais on peut montrer que, en modifiant légèrement r et θ, on peut faire acquérir à $f(z)$ un module inférieur à R, si R n'est pas nul. Si l'on remplace z_0 par $z_0 + h$ où

$$h = \rho\omega,$$

on a

$$f(z_0 + h) = f(z_0) + f^p(z_0)\frac{h^p}{p!} + f^{p+1}(z_0)\frac{h^{p+1}}{(p+1)!} + \ldots + A_0 h^n,$$

où p peut être $\overline{\gtrless} 1$, plusieurs dérivées pouvant être nulles. On a alors

$$\frac{f(z_0+h)}{f(z_0)} = 1 + C_p \rho^p[\cos(p\omega + \alpha_p) + i\sin(p\omega + \alpha_p)] + B,$$

B étant divisible par une puissance de ρ supérieure à p, en posant

$$\frac{f^p(z_0)}{p!\,f(z_0)} = C_p(\cos\alpha_p + i\sin\alpha_p).$$

Si l'on choisit ω de telle sorte que $p\omega + \alpha_p = \pi$, on a

$$\cos(p\omega + \alpha_p) = -1, \qquad \sin(p\omega + \alpha_p) = 0$$

et

$$\frac{f(z_0+h)}{f(z_0)} = 1 - C_p\rho^p + B_0,$$

où B_0 est la valeur que prend B pour la valeur assignée à ω. Le terme $-C_p\rho^p$ est négatif et, pour de petites valeurs numériques de ρ, supérieur au module de B_0 : on peut donc prendre ω et ρ tels que

$$\operatorname{mod}\frac{f(z_0+h)}{f(z_0)} < 1 \qquad \text{ou} \qquad \operatorname{mod} f(z_0+h) < \operatorname{mod} f(z_0).$$

Le minimum de R est donc zéro et le théorème est démontré.

On pourrait cependant objecter que R, en décroissant, pourrait tendre vers une limite différente de zéro sans l'atteindre; mais, si l'on considère les valeurs de R correspondant aux valeurs finies de z, il y en aura une qui sera minima; mais cela est impossible, comme on l'a vu, si cette valeur minima n'est pas nulle. Il reste donc à montrer que z ne croît pas indéfiniment quand R tend vers zéro. Or, cela n'a évidemment pas lieu puisque $f(z)$ croît indéfiniment avec z.

Racines conjuguées des équations à coefficients réels.

12. *Si la quantité imaginaire $a+bi$ est racine d'une équation à coefficients réels, $a-bi$ est également racine de cette équation.*

En effet, on a, en désignant par $f(z)$ un polynome entier et par $a+bi$ une racine de $f(z)=0$,

$$f(z)=[z-(a+bi)]Q,$$

Q désignant un polynome entier. Comme $f(z)$ ne contient pas i, i doit disparaître du second membre après que l'on y aura effectué la multiplication, ce qui ne peut avoir lieu que si les exposants de i sont tous pairs, et alors son expression ne doit pas changer quand on remplace i par $-i$; il en résulte que

$$f(z)=[z-(a-bi)]Q_1,$$

où Q_1 est entier et ne diffère de Q que par le changement de i en $-i$; on voit donc que $f(z)$ est divisible par $z-(a-bi)$ ou que $a-bi$ est également racine de $f(z)=0$.

Les racines imaginaires d'une équation à coefficients réels sont donc en nombre pair et les facteurs imaginaires du premier degré d'un polynome entier à coefficients réels sont, par suite, également en nombre pair.

En groupant deux facteurs imaginaires conjugués, on obtient le facteur réel

$$(z - a)^2 + b^2.$$

On voit donc qu'un polynome entier à coefficients réels peut se décomposer en facteurs réels du premier et du second degré.

Détermination de la racine commune à deux équations.

13. Si les deux équations $f(z) = 0$ et $F(z) = 0$ ont les racines communes $a, b, c, \ldots, f(z)$ et $F(z)$ auront le facteur commun $(z - a)(z - b)(z - c)\ldots$ et *vice versa*. Comme on peut toujours obtenir, par des méthodes connues, le facteur commun à deux polynomes, on pourra toujours trouver une équation ayant pour racines les racines communes à deux équations données. Des équations ayant des racines communes pourront donc toujours être remplacées par d'autres de degré moins élevé. Si, par exemple, $\varphi(z)$ est le plus grand commun diviseur de $f(z)$ et $F(z)$, l'équation $\varphi(z) = 0$ aura pour racines les racines communes à $f(z) = 0$ et $F(z) = 0$. Les autres racines de ces équations satisferont aux équations

$$\frac{f(z)}{\varphi(z)} = 0, \qquad \frac{F(z)}{\varphi(z)} = 0.$$

Si les équations données avaient des racines multiples communes, $\varphi(z) = 0$ admettrait ces racines avec leur plus petit degré de multiplicité. Si, par exemple, $f(z)$ est divisible par $(z - \alpha)^p$ et $F(z)$ par $(z - \alpha)^{p+q}$, $\varphi(z)$ l'est par $(z - \alpha)^p$, $F(z):\varphi(z)$ et $\varphi(z)$ auront donc encore des racines communes et leur degré pourra être encore abaissé, etc.

Une équation $f(z) = 0$ à coefficients numériques rationnels est dite *irréductible* quand $f(z)$ ne peut pas se décomposer en facteurs à coefficients rationnels. Cette notion peut être généralisée; si l'on regarde certains nombres irrationnels comme donnés, adjoints, comme l'on dit, on peut les

considérer comme rationnels. L'équation $z^2 - 3 = 0$ est alors irréductible dans le sens primitif du mot, mais elle devient réductible après l'adjonction du radical $\sqrt{3}$: le domaine de rationalité ordinaire est alors étendu, comme l'on dit, à $\sqrt{3}$.

Si les coefficients contiennent des irrationnelles, il faut les considérer comme adjoints.

Si les coefficients contiennent des lettres, on doit les considérer comme des quantités rationnelles. Des fonctions irrationnelles de lettres peuvent être adjointes. Ordinairement, quand les coefficients contiennent des lettres, on adjoint toutes les irrationnelles numériques.

Comme $\varphi(z)$ est rationnel quand $f(z)$ et $F(z)$ le sont euxmêmes, on voit que deux équations sont réductibles, quand elles ont des racines communes; cependant il pourra arriver que $f(z)$ divise $F(z)$ et que $\varphi(z) = f(z)$; dans ce cas $f(z) = 0$ pourrait être irréductible.

Il résulte de là que, *quand une équation admet une racine d'une équation irréductible, elle les admet toutes.*

Condition pour que deux équations aient des racines communes.

14. Proposons-nous de trouver la condition nécessaire et suffisante que doivent remplir les coefficients de deux équations, pour qu'elles aient des racines communes.

Soient les équations

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_n = 0, \tag{1}$$

$$f_1(z) = z^m + b_1 z^{m-1} + b_2 z^{m-2} + \ldots + b_m = 0. \tag{2}$$

Si ces deux équations ont une racine commune, $f(z)$ et $f_1(z)$ ont un diviseur commun; si l'on cherche le plus grand commun diviseur de $f(z)$ et $f_1(z)$, on finit par trouver un reste qui n'est fonction que des coefficients des deux équations; soit V ce reste, d'où l'on a éliminé les facteurs introduits pour faciliter la division s'il y a lieu.

$$V = 0 \tag{3}$$

sera la condition nécessaire et suffisante pour que nos équations aient une solution commune, le reste qui précède a la forme

$$V_1 z + V_2;$$

s'il est identiquement nul, les polynomes f et f_1 ont un facteur commun du deuxième degré, et les équations proposées ont deux racines communes; la condition pour que les équations en question aient deux racines communes est donc

$$(4) \qquad V_1 = 0, \qquad V_2 = 0,$$

et ainsi de suite.

15. Lagrange a mis ces équations de condition sous une forme différente. Supposons un des coefficients des équations a variable, les autres restant constants; quand a varie d'une manière continue, on peut admettre que les racines varient également d'une manière continue [1]; demandons-nous quel accroissement h il faut donner à a pour que l'équation (1), dans sa nouvelle forme, ait une racine commune avec (2). Si dans V on change a en $a + h$, cette expression devient

$$(5) \qquad V_h = V + \frac{dV}{da} h + \frac{d^2 V}{da^2} \frac{h^2}{1.2} + \ldots.$$

Si la quantité a est déterminée de telle sorte que les équations (1), (2) aient une racine commune, on a $V = 0$; si, pour $a + h$, on a encore une racine commune, on a, en outre, $V_h = 0$; l'accroissement h est alors donné par la formule

$$(6) \qquad \frac{dV}{da} h + \frac{d^2 V}{da^2} \frac{h^2}{1.2} + \frac{d^3 V}{da^3} \frac{h^3}{1.2.3} + \ldots = 0.$$

Si l'on remplace dans (1) z par toutes les racines de (2), a reçoit, pour chacune d'elles, une valeur correspondante qui satisfait à (1), et à chacune de ces valeurs de a correspond,

---

[1] Cela résulte de l'existence des dérivées des fonctions implicites.

dans (6), une valeur de h. Ces m valeurs de h correspondent chacune à une racine de (2). D'un autre côté, deux équations (1), qui correspondent à des valeurs distinctes de a, ne peuvent avoir de racines communes (excepté si $z=0$, cas que l'on peut laisser de côté). Si alors, pour une valeur de a, q racines de l'équation (2) satisfont à (1), q des racines de (6) doivent être nulles. Donc *la condition nécessaire et suffisante pour que q racines de* (2) *satisfassent à* (1) *est*

$$(7)\quad V=0,\qquad \frac{dV}{da}=0,\qquad \frac{d^2V}{da^2}=0,\qquad \ldots,\qquad \frac{d^{q-1}V}{da^{q-1}}=0,$$

en sous-entendant que $z=0$ n'est pas racine.

Ces équations sont équivalentes à celles qui ont été trouvées plus haut si les q racines sont distinctes; si α était plusieurs fois racine de (2), il n'a besoin que d'être racine simple de (1) pour que les équations (7) aient lieu. On voit que, au lieu de supposer a égal à l'un des coefficients de (1), on pourrait le supposer choisi de telle sorte que les coefficients de (1) soient fonctions linéaires de ce paramètre; cette équation serait alors de la forme $A+aB=0$ et, d'après ce que l'on a vu plus haut, il faudrait supposer que A et B n'ont pas de facteur commun.

Racines égales.

16. *Toute quantité p fois racine de $f(z)=0$ est exactement racine de $f'(z)=0$.*

Soit, en effet, α une racine d'ordre de multiplicité p de $p-1$ *fois* $f(z)=0$, alors on a

$$f(z)=(z-\alpha)^pQ,$$

où Q n'admet plus le facteur $(z-\alpha)$. On en tire

$$\begin{aligned} f'(z) &= p(z-\alpha)^{p-1}Q+(z-\alpha)^pQ' \\ &= (z-\alpha)^{p-1}[pQ+(z-\alpha)Q']. \end{aligned}$$

Q' désignant la dérivée de Q; $f'(z)$ est donc divisible par $(z-\alpha)^{p-1}$ et n'est pas divisible par une puissance plus élevée

de $z-\alpha$, puisque pQ n'est pas divisible par $z-\alpha$. α est donc racine d'ordre de multiplicité $p-1$ de $f'(z)$.

Désignons maintenant par P_1 le produit des facteurs simples de $f(z)$, par P_2 le produit des facteurs doubles pris une seule fois, etc., en sorte que

$$f(z)=P_1P_2^2P_3^3\ldots,$$
$$f'(z)=P_2P_3^2\ldots Q,$$

Q désignant les facteurs de $f'(z)$ non contenus dans $f(z)$; le plus grand commun diviseur de $f(z)$ et $f'(z)$ sera

$$\varphi(z)=P_2P_3^2\ldots,$$

d'où

$$\frac{f(z)}{\varphi(z)}=P_1P_2P_3\ldots=f_1(z).$$

En appelant $\varphi_1(z)$ le plus grand commun diviseur de $\varphi(z)$ et de $\varphi'(z)$, on trouve, en divisant $\varphi(z)$ par $\varphi_1(z)$,

$$f_2(z)=P_2P_3\ldots;$$

donc

$$\frac{f_1(z)}{f_2(z)}=P_1.$$

On a ainsi l'expression

$$P_1=0$$

de l'équation à laquelle satisfont les racines simples de $f(z)=0$. Cette équation est, en général, irréductible. Pour déterminer P_2, on a

$$\varphi_1(z)=P_3P_4^2\ldots,$$

et si $\varphi_2(z)$ est le plus grand commun diviseur de $\varphi_1(z)$ et de $\varphi'_1(z)$, on a

$$\frac{\varphi_1(z)}{\varphi_2(z)}=P_3P_4\ldots=f_3(z),$$

d'où l'on tire

$$\frac{f_2(z)}{f_3(z)}=P_2.$$

En continuant ainsi, on a successivement

$$P_1 = 0, \quad P_2 = 0, \quad P_3 = 0, \quad \ldots$$

et la résolution de ces équations fait connaître les racines de $f(z) = 0$. On ne saura pas toujours résoudre ces équations, mais en tout cas, *il est toujours possible de remplacer la résolution d'une équation qui a des racines multiples par la résolution d'autres équations qui n'ont que des racines simples et lesquelles entrent à un même degré de multiplicité dans* $f(z) = 0$.

Expression des coefficients en fonction des racines.

17. La forme la plus générale de l'équation du degré n, quand on divise le premier membre par le coefficient de z^n, est

$$(1) \qquad f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_{n-1} z + a_n = 0,$$

et si l'on désigne par $\alpha_1, \alpha_2, \ldots, \alpha_n$ ses racines, on a

$$(2) \qquad f(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n).$$

Si l'on effectue le produit indiqué dans le second membre de cette équation, et si on l'identifie avec le développement de $f(z)$, on obtient les formules

$$(3) \qquad \left\{ \begin{array}{l} \alpha_1 + \alpha_2 + \ldots + \alpha_n = -a_1, \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n = a_2, \\ \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n = -a_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \alpha_1\alpha_2\ldots\alpha_n = (-1)^n a_n. \end{array} \right.$$

CHAPITRE II.

RELATIONS ENTRE LES COEFFICIENTS ET LES RACINES.

Fonctions symétriques des racines.

18. Une fonction de plusieurs variables est dite *symétrique* quand elle reste invariable lorsque l'on permute deux de ces variables d'une façon quelconque. Nous ne considérerons dans la suite que des fonctions symétriques rationnelles. Quand une expression de forme non symétrique ne change pas de valeur, quand on y permute les lettres qu'elle renferme, pour des valeurs déterminées de ces lettres, on peut lui donner une forme symétrique. Ainsi, par exemple,

$$a^2 + 3b,$$

pour $a = 1$ et $b = 2$, ne change pas de valeur quand on permute a et b; on peut l'écrire sous la forme symétrique

$$\frac{1}{2}(a^2 + 3b + b^2 + 3a).$$

D'une manière générale, si φ ne change pas de valeur, en permutant certaines quantités données, et si, par les permutations de ces quantités, elle prend les formes $\varphi_1, \varphi_2, \ldots, \varphi_n$, on peut poser

$$\varphi = \frac{1}{n}(\varphi_1 + \varphi_2 + \ldots + \varphi_n),$$

et φ prend la forme symétrique.

Une fonction quelconque symétrique des racines d'une

équation peut s'exprimer rationnellement en fonction des coefficients.

Dans le cas où la fonction est fractionnaire, on peut la mettre sous une forme telle que le numérateur et le dénominateur soient symétriques. Si, en effet, on considérait la fraction réduite à sa plus simple expression

$$\frac{\varphi(x_1, x_2, \ldots)}{\psi(x_1, x_2, \ldots)},$$

et si les deux termes n'étaient pas des fonctions symétriques, il y aurait deux valeurs x_1 et x_2, qui, en s'échangeant, laisseraient inaltérée la valeur de la fraction, tandis que les valeurs du numérateur et du dénominateur se trouveraient changées. Mais cela est impossible, car il en résulterait deux fractions égales, capables de devenir infinies pour des valeurs de x_1, x_2, ... qui ne seraient pas les mêmes.

On peut donc, si l'on veut, ne considérer que des fonctions symétriques entières. Considérons un terme d'une telle fonction, et permutons les racines qui y entrent de toutes les manières possibles : les résultats devront entrer dans la fonction symétrique et leur somme sera symétrique; les autres termes peuvent être traités de la même façon.

Considérons, par exemple, une équation du troisième degré ayant pour racines x_1, x_2, x_3. Si, dans une fonction symétrique des racines, il entre le terme $x_1 x_2^2 x_3$, il doit aussi y entrer les termes $x_2 x_1^2 x_3$, $x_1 x_3^2 x_2$, et l'on aura à considérer la fonction

$$x_1 x_2^2 x_3 + x_2 x_1^2 x_3 + x_1 x_3^2 x_2,$$

qui peut s'écrire

$$x_1 x_2 x_3 (x_1 + x_2 + x_3),$$

et l'on a alors affaire aux fonctions $x_1 x_2 x_3$ et $x_1 + x_2 + x_3$; en réalité, on aurait dû obtenir six termes, car le nombre des permutations de trois lettres est 6; mais le terme considéré est lui-même symétrique par rapport à deux racines : il n'y a pour cette raison que trois permutations donnant des résultats différents.

Ainsi, une fonction symétrique, qui ne peut pas être décomposée en fonctions plus simples, est déterminée par un seul de ses termes; on la représente par ce terme, précédé du signe Σ; par exemple, pour une équation de degré n,

$$\Sigma x_1 x_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + \ldots + x_{n-1} x_n,$$
$$\Sigma x_1^2 = x_1^2 + x_2^2 + x_3^2 + \ldots + x_n^2.$$

Formules de Newton.

19. Nous considérerons, en particulier, les fonctions symétriques

$$\Sigma x_1 = s_1, \qquad \Sigma x_1^2 = s_2, \qquad \ldots, \qquad \Sigma x_1^r = s_r,$$

pour le calcul desquelles Newton a donné la méthode suivante : de

$$(1) \qquad f(x) = (x - x_1)(x - x_2)\ldots(x - x_n)$$

on tire, en prenant les dérivées logarithmiques [1],

$$(2) \qquad \frac{f'(x)}{f(x)} = \frac{1}{x - x_1} + \frac{1}{x - x_2} + \ldots + \frac{1}{x - x_n}.$$

---

[1] Cette formule peut aussi s'établir comme il suit : on tire de

$$f(x) = (x - x_1)(x - x_2)\ldots(x - x_n)$$

la formule

$$f(x + h) = (x + h - x_1)(x + h - x_2)\ldots(x + h - x_n)$$

et

$$\frac{f(x + h)}{f(x)} = \left(1 + \frac{h}{x - x_1}\right)\left(1 + \frac{h}{x - x_2}\right)\cdots\left(1 + \frac{h}{x - x_n}\right);$$

mais

$$\frac{f(x + h)}{f(x)} = 1 + \frac{f'(x)}{f(x)}\frac{h}{1} + \frac{f''(x)}{f(x)}\frac{h^2}{1.2} + \ldots;$$

si l'on égale les coefficients des mêmes puissances de h dans les deux expressions de $\frac{f(x + h)}{f(x)}$; on a

$$\frac{f'(x)}{f(x)} = \frac{1}{x - x_1} + \frac{1}{x - x_2} + \ldots + \frac{1}{x - x_n},$$

$$\frac{1}{2}\frac{f''(x)}{f(x)} = \frac{1}{(x - x_1)(x - x_2)} + \frac{1}{(x - x_1)(x - x_3)} + \ldots + \frac{1}{(x - x_{n-1})(x - x_n)},$$

....

Ainsi

$$(3)\qquad f'(x) = \frac{f(x)}{x-x_1} + \frac{f(x)}{x-x_2} + \ldots + \frac{f(x)}{x-x_n};$$

or on a

$$(4)\qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$

et

$$\frac{f(x)}{x-x_1} = \begin{array}{r|r|r|r} x^{n-1} + x_1 & x^{n-2} + x_1^2 & x^{n-3} + x_1^3 & x^{n-4} + \ldots + x_1^{n-1} \\ + a_1 & + a_1 x_1 & + a_1 x_1^2 & + a_1 x_1^{n-2} \\ & + a_2 & + a_2 x_1 & + a_2 x_1^{n-3} \\ & & + a_3 & + \ldots\ldots \\ & & & + a_{n-2} x_1 \\ & & & + a_{n-1}; \end{array}$$

on a d'autres équations analogues, en permutant x_1 avec les autres racines $x_2, x_3, \ldots, x_n$.

En ajoutant toutes ces formules, on a, avec les notations adoptées tout à l'heure,

$$f'(x) = \begin{array}{r|r|r|r} n x^{n-1} + s_1 & x^{n-2} + s_2 & x^{n-2} + s_3 & x^{n-3} + \ldots + s_{n-1} \\ + n a_1 & + a_1 s_1 & + a_1 s_2 & + a_1 s_{n-2} \\ & + n a_2 & + a_2 s_1 & + a_2 s_{n-3} \\ & & + n a_3 & + \ldots\ldots \\ & & & + a_{n-2} s_1 \\ & & & + n a_{n-1}; \end{array}$$

d'un autre côté,

$$(5)\qquad f'(x) = n x^{n-1} + (n-1) a_1 x^{n-2} + (n-2) a_2 x^{n-3} + \ldots + a_{n-1};$$

en identifiant les deux valeurs de $f'(x)$, on a

$$(6)\qquad \left\{ \begin{array}{l} s_1 + a_1 = 0, \\ s_2 + a_1 s_1 + 2 a_2 = 0, \\ s_3 + a_1 s_2 + a_2 s_1 + 3 a_3 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ s_{n-1} + a_1 s_{n-2} + a_2 s_{n-3} + \ldots + a_{n-2} s_1 + (n-1) a_{n-1} = 0. \end{array} \right.$$

De ces équations on tire, par un calcul de proche en proche,

$$(7)\quad \begin{cases} s_1 = -a_1, \\ s_2 = a_1^2 - 2a_2, \\ s_3 = -a_1^3 + 3a_1a_2 - 3a_3, \\ s_4 = a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 - 4a_4, \\ s_5 = -a_1^5 + 5a_1^3a_2 - 5a_1^2a_3 - 5(a_2^2 - a_4)a_1 + 5a_2a_3 - 5a_5, \\ \dots\dots\dots\dots\dots\dots\dots\dots ; \end{cases}$$

ces formules ne peuvent servir qu'à calculer $s_1, s_2, \dots, s_{n-1}$. Pour calculer $s_n, s_{n+1}, \dots$, on multiplie $f(x) = 0$ par x^m, et l'on a

$$x^{n+m} + a_1x^{n+m-1} + a_2x^{n+m-2} + \dots + a_nx^m = 0,$$

équation satisfaite pour $x = x_1, x_2, \dots, x_n$. Si l'on remplace successivement x par ces valeurs, et si l'on ajoute les résultats obtenus, on trouve

$$(8)\qquad s_{n+m} + a_1s_{n+m-1} + a_2s_{n+m-2} + \dots + a_ns_n = 0,$$

et, en faisant $m = 0, 1, 2, \dots$ (et en observant que $s_0 = n$), on a

$$(9)\quad \begin{cases} s_n \phantom{{}_{+1}} + a_1s_{n-1} + a_2s_{n-2} + \dots + na_n = 0, \\ s_{n+1} + a_1s_n \phantom{{}_{+1}} + a_2s_{n-1} + \dots + a_ns_1 = 0, \\ s_{n+2} + a_1s_{n+1} + a_2s_n \phantom{{}_{+1}} + \dots + a_ns_2 = 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots \end{cases}$$

Ces formules permettent de calculer $s_n, s_{n+1}, s_{n+2}, \dots$ quand $s_{n-1}, s_{n-2}, \dots$ ont été calculés par les formules précédentes. Les formules, auxquelles nous venons de parvenir, montrent que, si les coefficients de l'équation (4) sont des nombres entiers, les sommes des puissances semblables des racines sont aussi des nombres entiers. Dans la suite, nous aurons besoin de remarquer que les formules précédentes sont homogènes, quand on y considère les indices des a et des s, comme jouant le rôle d'exposants. Enfin que les coefficients sont donnés par des équations linéaires quand on connaît

$$s_1, \quad s_2, \quad \dots, \quad s_n.$$

Quand on connaît s_p pour n valeurs de p consécutives, on détermine les coefficients à l'aide de n équations.

Le calcul de s_{-p} peut se faire en faisant usage de l'équation obtenue en changeant x en $\frac{1}{x}$; pour celle-ci on a, en effet,

$$S_p = \sum \left(\frac{1}{x}\right)^p = \sum x_1^{-p} = s_{-p}.$$

20. On peut encore obtenir s_p de la manière suivante : on a

$$\frac{1}{x - x_p} = \frac{1}{x} + \frac{x_p}{x^2} + \frac{x_p^2}{x^3} + \ldots; \tag{10}$$

cette équation a lieu en supposant le module de x supérieur au plus grand des modules des racines, afin que le second membre soit convergent; si l'on remplace alors x_p successivement par toutes les racines de l'équation et, si l'on ajoute, on obtient, en vertu de la formule (2) du n° 19,

$$\frac{f'(x)}{f(x)} = \frac{n}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \ldots,$$

$$\frac{x\, f'(x)}{f(x)} = n + \frac{s_1}{x} + \frac{s_2}{x^2} + \ldots. \tag{11}$$

Si l'on développe alors le premier membre, suivant les puissances de $\frac{1}{x}$, on obtient deux expressions de cette fonction qui doivent être identiques pour les valeurs de x de module supérieur à une quantité déterminée. Une simple division permettra donc de calculer s_1, s_2, ...

La quantité $\frac{1}{x - x_1}$ peut aussi, pour des valeurs suffisamment petites de x, se développer en série convergente, suivant les puissances de x à exposants positifs ; on a

$$\frac{1}{x - x_1} = -\left(\frac{1}{x_1} + \frac{x}{x_1^2} + \frac{x^2}{x_1^3} + \ldots\right);$$

on en déduit, par des moyens analogues à celui qui a été

employé tout à l'heure,

$$(12) \qquad -\frac{f'(x)}{f(x)} = s_{-1} + s_{-2}x + s_{-3}x^2 + \ldots,$$

et l'on trouve s_{-1}, s_{-2}, ... en ordonnant le quotient $\frac{f'(x)}{f(x)}$, suivant les puissances positives de x. On voit l'identité des méthodes qui ont permis de calculer s_p en fonction de s_{p-1}, s_{p-2}, ..., s_{p-n}, à l'aide de la formule (9) du n° 19, et qui permettent de calculer un terme d'une série récurrente en fonction des précédents; les termes de l'échelle de relation sont les coefficients de l'équation changés de signe.

Autres fonctions symétriques.

21. Les fonctions symétriques que nous venons d'apprendre à calculer sont ce que l'on appelle les *fonctions simples;* les fonctions doubles sont celles dans chacun des termes desquelles il entre deux racines, les fonctions triples sont celles dont les termes en contiennent trois, etc.

Le terme général d'une fonction double est ainsi de la forme $x_1^\alpha x_2^\beta$. Si l'on forme le produit $s_\alpha s_\beta$, on trouve les termes de $\Sigma x_1^\alpha x_2^\beta$, et, en outre, des termes de la forme $x_1^{\alpha+\beta}$; ainsi on a

$$(1) \qquad \Sigma x_1^\alpha x_2^\beta = s_\alpha s_\beta - s_{\alpha+\beta};$$

on voit que les fonctions doubles seront des nombres entiers si les coefficients eux-mêmes sont entiers, et que leur degré, estimé comme nous l'avons dit plus haut, est égal à la somme des exposants α, β.

Pour $\alpha = \beta$, les termes sont égaux deux à deux, car $x_1^\alpha x_2^\alpha = x_2^\alpha x_1^\alpha$; et comme, dans la fonction symétrique, ces termes ne figurent qu'une fois, on a

$$\Sigma x_1^\alpha x_2^\alpha = \frac{1}{2}(s_\alpha^2 - s_{2\alpha}).$$

Pour obtenir la fonction symétrique triple $\Sigma x_1^\alpha x_2^\beta x_3^\gamma$, on multiplie (1) par s_γ, et l'on a

$$s_\gamma \Sigma x_1^\alpha x_2^\beta = s_\alpha s_\beta s_\gamma - s_{\alpha+\beta} s_\gamma.$$

Les termes du premier membre contiennent ceux de la fonction symétrique cherchée, mais il y en a d'autres qui proviennent de la multiplication de termes de la forme x_1^γ par des termes contenant encore x_1; ces termes sont ceux de la fonction symétrique

$$\Sigma x_1^{\alpha+\gamma} x_2^\beta + \Sigma x_1^\alpha x_2^{\beta+\gamma} = s_\beta s_{\alpha+\gamma} + s_\alpha s_{\beta+\gamma} - 2 s_{\alpha+\beta+\gamma};$$

on a donc

$$(3)\quad \Sigma x_1^\alpha x_2^\beta x_3^\gamma = s_\alpha s_\beta s_\gamma - s_\alpha s_{\beta+\gamma} - s_\beta s_{\alpha+\gamma} - s_\gamma s_{\alpha+\beta} + 2 s_{\alpha+\beta+\gamma},$$

dans le cas où deux des exposants α, β, γ deviennent égaux, les termes deviennent égaux deux à deux; quand les trois exposants α, β, γ deviennent égaux, six termes deviennent égaux; ainsi on a

$$(4)\qquad \Sigma x_1^\alpha x_2^\alpha x_3^\gamma = \frac{1}{2}(s_\alpha^2 s_\gamma - 2 s_\alpha s_{\alpha+\gamma} - s_{2\alpha} s_\gamma + 2 s_{2\alpha+\gamma}),$$

$$(5)\qquad \Sigma x_1^\alpha x_2^\alpha x_3^\alpha = \frac{1}{2.3}(s_\alpha^3 - 3 s_\alpha s_{2\alpha} + 2 s_{3\alpha}).$$

On peut continuer ainsi, et il est démontré que *toute fonction symétrique entière des racines est une fonction entière des coefficients;* elle est homogène, et son degré est la somme des exposants des racines, pourvu que l'on considère a_p comme étant du degré p.

Nouvelle méthode pour le calcul des fonctions symétriques des racines.

22. Les formules de Newton s'appliquent assez facilement aux équations numériques, mais il y a d'autres méthodes qui sont préférables quand l'on a affaire à des équations littérales. Telles sont les méthodes de Waring et de Cauchy; nous

allons indiquer ici une méthode qui, au fond, coïncide avec celle de Waring, mais qui est d'une application plus commode.

Pour la facilité de l'exposition, nous écrirons l'équation donnée sous la forme

$$(1) \qquad x^n - a_1 x^{n-1} + a_2 x^{n-2} - a_3 x^{n-3} + \ldots = 0,$$

nous supposerons la fonction symétrique φ de degré α; soit

$$(2) \qquad \varphi = A_{\alpha-n} a_n + A_{\alpha-n+1} a_{n-1} + \ldots,$$

$A_{\alpha-n} a_n$ contient tous les termes de φ qui dépendent de a_n; $A_{\alpha-n+1} a_{n-1}$ contient, parmi ceux qui restent, tous ceux qui dépendent de a_{n-1}, etc., l'indice est égal au degré. Cette équation, quand on y remplace a_n, a_{n-1}, ... par leurs valeurs en fonction des racines, se transforme en une identité; on peut y annuler autant de racines que l'on veut, et si l'on s'arrange de telle sorte que le dernier terme de φ, en faisant cela, soit le seul qui ne soit pas nul, ce terme sera tout calculé; on peut alors se débarrasser par la division du produit des racines restantes, et continuer à appliquer la même méthode. Nous allons appliquer cette méthode à quelques exemples.

Exemple I :

$$(3) \qquad \Sigma x_1^3 x_2^2 x_3 = A_0 a_6 + A_1 a_5 + A_2 a_4 + A_3 a_3;$$

le premier terme contient a_6 puisque Σ est du sixième degré; ce terme disparaîtrait si la fonction était de degré moindre. Le dernier terme contient a_3, car la fonction s'annule si l'on annule toutes les racines sauf deux.

Posons maintenant

$$x_4 = x_5 = x_6 = \ldots = 0;$$

alors on a

$$(4) \qquad \Sigma x_1^3 x_2^2 x_3 = A_3 a_3.$$

Nous pouvons conserver notre notation primitive, en nous rappelant que l'indice le plus élevé est 3; en divisant par $x_1 x_2 x_3$, on a

$$(5) \qquad \Sigma x_1^2 x_2 = A_3 = \alpha_0 a_3 + \alpha_1 a_2 a_1;$$

a_1^3 n'entre pas dans A_3, car la fonction doit s'annuler quand deux racines s'annulent.

Si l'on pose $x_3 = 0$, on trouve

$$x_1 x_2 \Sigma x_1 = \alpha_1 a_2 a_1, \qquad \alpha_1 = 1;$$

et de (5)

$$\alpha_0 = \frac{\Sigma x_1^2 x_2 - a_1 a_2}{x_1 x_2 x_3}.$$

Comme cette formule est identique, on peut y faire toutes les racines égales à l'unité, alors tous les produits de racines qui se rencontrent dans la fraction se réduisent à l'unité, et l'on a

$$\alpha_0 = 6 - 3.3 = -3.$$

Si maintenant on fait $x_p = 0$ pour $p > 4$,

$$\Sigma x_1^3 x_2^2 x_3 = A_2 a_4 - 3a_3^2 + a_1 a_2 a_3$$

ou

$$\frac{\Sigma x_1^3 x_2^2 x_3 + 3a_3^2 - a_1 a_2 a_3}{x_1 x_2 x_3 x_4} = A_2 = \alpha_0 a_2 + \alpha_1 a_1^2,$$

formule où α_0 et α_1 sont à déterminer. Pour y arriver, posons trois racines égales à l'unité et la quatrième égale à h; cherchons le coefficient de h^2 dans le second membre pour l'égaler au coefficient de h^3 dans le numérateur du premier; dans $\Sigma x_1^3 x_2^2 x_3$, on n'utilisera que les termes qui ont l'exposant 3 en h, et l'on trouvera ainsi h^3 autant de fois qu'il est possible de prendre deux racines parmi les trois que l'on a fait égales à un, c'est-à-dire six fois; alors, comme on a

$$a_3 = 1 + 3h, \qquad a_2 = 3 + 3h, \qquad a_1 = h + 3,$$

on a

$$6 - 9 = \alpha_1 = -3;$$

et, en prenant toutes les racines égales à l'unité,

$$24 + 48 - 96 = 6\alpha_0 - 3.16,$$

$$\alpha_0 = 4;$$

on a donc maintenant

$$\frac{\Sigma x_1^3 x_2^2 x_3 - a_4(4a_2 - 3a_1^2) + 3a_3^2 - a_1 a_2 a_3}{x_1 x_2 x_3 x_4 x_5} = A_1 = \alpha a_1,$$

si l'on annule toutes les racines sauf 5. Et si l'on prend ces cinq racines égales à l'unité, on a

$$60 - 5(4.10 - 3.25) + 3.10^2 - 5.10.10 = \alpha.5,$$
$$\alpha = 7,$$

et finalement $A_0 = -12$, de sorte que le résultat pour toute équation sera

$$\Sigma x_1^3 x_2^2 x_3 = -12 a_6 + 7 a_5 a_1 + a_4(4 a_2 - 3 a_1^2) - 3 a_3^2 + a_1 a_2 a_3.$$

Exemple II. — Pour l'équation

$$x^3 - a_1 x^2 + a_2 x - a_3 = 0,$$

on demande de calculer

$$U = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2;$$

on a

$$U = A_3 a_3 + A_4 a_2,$$

les termes suivants doivent manquer, U s'annulant alors que deux racines deviennent égales à zéro.

Pour $x_3 = 0$, on a

$$x_1^2 x_2^2 (x_1 - x_2)^2 = A_4 a_2 = a_2^2(-4 a_2 + a_1^2);$$

et alors

$$U = a_3(\alpha_0 a_3 + \alpha_1 a_2 a_1 + \alpha_2 a_1^3) + a_2^2(-4 a_2 + a_1^2).$$

si l'on fait

$$x_1 = x_2 = 1, \qquad x_3 = h,$$

et si l'on égale les coefficients de h^4, on a

$$0 = \alpha_2 + 4, \qquad \alpha_2 = -4;$$

en égalant les coefficients de h^3, on a

$$2\alpha_1 - 24 - 12 = 0,$$
$$\alpha_1 = 18;$$

et si l'on égale toutes les racines à l'unité, on trouve

$$\alpha_0 = -27;$$

ainsi on a

$$U = -27 a_3^2 + 18 a_3 a_2 a_1 - 4 a_3 a_1^3 - 4 a_2^3 + a_2^2 a_1^2.$$

Dans cet exemple et dans le précédent, le résultat ne change pas en revenant à la forme primitive de l'équation avec tous les coefficients positifs.

Formules générales pour le calcul de s_p et de a_p.

23. Le théorème de Newton permet de calculer s_p quand les coefficients sont connus, et, inversement, les coefficients quand $s_1, s_2, \ldots, s_n$ sont donnés; mais le calcul exige la résolution d'un système d'équations linéaires. Par la méthode suivante, on trouve l'expression explicite de ces quantités.

Soit

$$(1)\quad (x - x_1)(x - x_2)\ldots(x - x_n) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n;$$

dans cette identité, supposons x plus grand que le plus grand des modules des racines; alors, en divisant par x^n et en prenant les logarithmes naturels, on a

$$(2)\quad \begin{cases} l\left(1 - \dfrac{x_1}{x}\right) + l\left(1 - \dfrac{x_2}{x}\right) + \ldots + l\left(1 - \dfrac{x_n}{x}\right) \\ \qquad = l\left(1 + \dfrac{a_1}{x} + \dfrac{a_2}{x^2} + \ldots + \dfrac{a_n}{x^n}\right); \end{cases}$$

tous les termes peuvent être développés en séries convergentes, et l'on a

$$(3)\quad -\left(\frac{s_1}{x} + \frac{s_2}{2x^2} + \ldots + \frac{s_p}{px^p} + \ldots\right) = \alpha - \frac{\alpha^2}{2} + \frac{\alpha^3}{3} - \frac{\alpha^4}{4} + \ldots,$$

formule où l'on a posé

$$\alpha = \frac{a_1}{x} + \frac{a_2}{x^2} + \ldots + \frac{a_n}{x^n}.$$

Égalons, de part et d'autre, les coefficients de x^{-p}; dans le premier membre, il est $-\dfrac{s_p}{p}$; dans le second membre, le terme général est

$$\frac{(-1)^{k+1}}{k}\left(\frac{a_1}{x} + \frac{a_2}{x^2} + \ldots + \frac{a_n}{x^n}\right)^k,$$

et le terme général du développement de la parenthèse est

égal (en vertu de la formule du polynome) à

$$(4)\qquad \frac{(\beta_1+\beta_2+\ldots+\beta_n)!}{\beta_1!\,\beta_2!\ldots\beta_n!}\,a_1^{\beta_1}a_2^{\beta_2}\ldots a_n^{\beta_n}.x^{-(\beta_1+2\beta_2+\ldots+n\beta_n)},$$

où

$$(5)\qquad \beta_1+\beta_2+\ldots+\beta_n=k;$$

on n'utilisera que les termes pour lesquels

$$(6)\qquad \beta_1+2\beta_2+\ldots+n\beta_n=p,$$

de sorte que la solution générale sera

$$(7)\quad s_p=\sum\frac{(-1)^{\beta_1+\beta_2+\ldots+\beta_n}p(\beta_1+\beta_2+\ldots+\beta_n-1)!}{\beta_1!\,\beta_2!\ldots\beta_n!}\,a_1^{\beta_1}a_2^{\beta_2}\ldots a_n^{\beta_n};$$

où β_1, β_2, ..., β_n doivent recevoir toutes les valeurs positives ou nulles satisfaisant à (6).

Pour obtenir a_p sous forme explicite, on tire de (2)

$$(8)\quad 1+\frac{a_1}{x}+\frac{a_2}{x^2}+\ldots+\frac{a_n}{x^n}=e^{-\left(\frac{s_1}{x}+\frac{s_2}{2x^2}+\ldots\right)}=1-\frac{\alpha}{1}+\frac{\alpha^2}{1.2}+\ldots$$

où

$$\alpha=\frac{s_1}{x}+\frac{s_2}{2x^2}+\frac{s_3}{3x^3}+\ldots,$$

et l'on trouve comme tout à l'heure

$$(9)\qquad a_p=\sum\frac{(-1)^{\beta_1+\beta_2+\ldots+\beta_n}}{\beta_1!\,\beta_2!\ldots\beta_n!}\left(\frac{s_1}{1}\right)^{\beta_1}\left(\frac{s_2}{2}\right)^{\beta_2}\ldots\left(\frac{s_p}{n}\right)^{\beta_n},$$

où

$$(10)\qquad \beta_1+2\beta_2+3\beta_3+\ldots+n\beta_n=p;$$

on trouve ainsi

$$(11)\quad\left\{\begin{aligned} a_1&=-s_1,\\ 2a_2&=\ \ s_1^2-s_2,\\ 3!\,a_3&=-s_1^3+3s_1s_2-2s_3,\\ 4!\,a_4&=\ \ s_1^4-6s_1^2s_2+8s_1s_3+3s_2^2-6s_4,\\ 5!\,a_5&=-s_1^5+10s_1^3s_2-20s_1^2s_3-15s_1s_2^2+30s_1s_4+20s_2s_3-24s_5,\end{aligned}\right.$$

comme avec les formules de Newton.

24. Si l'on applique (7) à l'équation

$$x^2 - ax + b = 0, \tag{12}$$

on trouve

$$s_p = \sum \frac{(-1)^\mu p(p-\mu-1)!}{(p-2\mu)!\,\mu!} a^{p-2\mu} b^\mu, \tag{13}$$

où μ doit recevoir toutes les valeurs 0, 1, 2, ... jusqu'au plus grand entier contenu dans $\frac{p}{2}$. On peut aussi écrire

$$(14) \quad \left\{ \begin{aligned} s_p &= a^p - pa^{p-2}b + \frac{p(p-3)}{1.2} a^{p-4} b^2 + \ldots \\ &\quad + (-1)^\mu \frac{p(p-\mu-1)(p-\mu-2)\ldots(p-2\mu+1)}{1.2.3\ldots\mu} a^{p-2\mu} b^\mu + \ldots; \end{aligned} \right.$$

pour l'équation

$$z^2 - zx + 1 = 0,$$

on a

$$(15) \quad \left\{ \begin{aligned} s_p &= x^p - px^{p-2} + \frac{p(p-3)}{1.2} x^{p-4} + \ldots \\ &\quad + (-1)^\mu \frac{p(p-\mu-1)(p-\mu-2)\ldots(p-2\mu+1)}{1.2.3\ldots\mu} x^{p-2\mu} + \ldots, \end{aligned} \right.$$

formule qui trouvera son application plus tard.

Équation aux carrés des différences.

25. Étant donnée une équation, on peut en déduire une autre dont les racines sont les carrés des différences des racines de la proposée. Soient

$$x_1, \quad x_2, \quad \ldots, \quad x_n$$

les racines de la proposée; les racines de l'équation cherchée seront

$$(x_1 - x_2)^2, \quad (x_1 - x_3)^2, \quad \ldots, \quad (x_{n-1} - x_n)^2,$$

et cette équation sera de degré $\frac{n(n-1)}{2}$.

Cette équation a joué autrefois un rôle important dans la théorie qui nous occupe. Si l'on annule son dernier terme, on exprime que la proposée a des racines égales, car cette circonstance exige qu'une des différences au moins soit nulle. Ce dernier terme, abstraction faite de son signe, porte le nom de *discriminant* de l'équation proposée. Si l'équation donnée a deux paires de racines égales $x_1 = x_2$, $x_3 = x_4$, les deux derniers termes de l'équation aux carrés des différences seront nuls. Si l'équation proposée a trois paires de racines égales, les trois derniers termes de l'équation aux carrés des différences seront nuls, etc.

L'équation aux carrés des différences servait surtout à trouver des intervalles comprenant une seule racine de l'équation proposée. Nous parlerons plus loin de cette application, nous allons donner ici une méthode simple pour former l'équation aux carrés des différences. Pour former cette équation, Lagrange exprime les sommes des puissances semblables de ses racines $S_1, S_2, \ldots$ en fonction des sommes des puissances semblables des racines $s_1, s_2, \ldots$ de la proposée comme il suit.

L'application de la formule du binome donne identiquement

$$(x - x_1)^{2p} + (x - x_2)^{2p} + \ldots + (x - x_n)^{2p}$$
$$= n x^{2p} - \frac{2p}{1} x^{2p-1} s_1 + \frac{2p(2p-1)}{1.2} x^{2p-2} s_2 + \ldots;$$

si l'on remplace successivement x par $x_1, x_2, \ldots$, et si l'on ajoute, on a

$$2S_p = n s_{2p} - \frac{2p}{1} s_{2p-1} s_1 + \frac{2p(2p-1)}{1.2} s_{2p-2} s_2 + \ldots + n s_{2p},$$

et comme les termes équidistants des extrêmes sont égaux,

$$(1) \quad S_p = n s_{2p} - \frac{2p}{1} s_{2p-1} s_1 + \ldots \pm \frac{1}{2} \frac{2p(2p-1)\ldots(p+1)}{1.2\ldots p} s_p^2.$$

Si, par exemple, l'équation donnée est

$$x^3 + p x^2 + q x + r = 0,$$

on trouve

$$S_1 = 3s_2 - s_1^2,$$
$$S_2 = 3s_4 - 4s_1s_3 + 3s_2^2,$$
$$S_3 = 3s_6 - 6s_1s_5 + 15s_2s_4 - 10s_3^2,$$

d'où l'on conclut l'équation aux carrés des différences

$$y^3 + Py^2 + Qy + R = 0$$

où

$$P = -2p^2 + 6q,$$
$$Q = p^4 - 6p^2q + 9q^2,$$
$$R = 4p^3r - p^2q^2 - 18pqr + 4q^3 + 27r^2.$$

On peut donner du discriminant une expression qui est souvent commode; si l'on pose

$$f(x) = (x - x_i)\varphi(x),$$

si l'on différentie et si l'on fait $x = x_i$, on trouvera

$$f'(x_i) = (x_i - x_1)(x_i - x_2)\ldots(x_i - x_{i-1})(x_i - x_{i+1})\ldots(x_i - x_n).$$

Si l'on remplace x_i successivement par toutes les racines et si l'on multiplie entre elles toutes les équations obtenues, on obtient dans le second membre tous les facteurs de la forme $-(x_i - x_j)^2$; le discriminant est donc de la forme

$$f'(x_1)f'(x_2)\ldots f'(x_n).$$

Fonctions rationnelles des racines.

26. Une fonction rationnelle d'une racine x_1 d'une équation $f(x) = 0$, de degré n, peut se mettre sous la forme

$$\frac{\varphi(x_1)}{\psi(x_1)} \tag{1}$$

φ et ψ désignant des polynomes entiers. Si l'on multiplie haut et bas par $\psi(x_2)\psi(x_3)\ldots\psi(x_n)$, on a

$$\varphi(x_1)\frac{\psi(x_2)\ldots\psi(x_n)}{\psi(x_1)\psi(x_2)\ldots\psi(x_n)}. \tag{2}$$

Le dénominateur est une fonction symétrique des racines et peut être exprimé rationnellement en fonction des coefficients; le numérateur est une fonction symétrique des racines de

$$(3) \qquad \frac{f(x)}{x - x_1} = 0,$$

dont les coefficients, quand on a effectué la division indiquée, sont des fonctions entières de x_1 et des coefficients de $f(x)$. La fonction rationnelle donnée est donc réductible à une fonction algébrique entière de x_1, j'ajoute que l'on peut supposer son degré au plus égal à $n - 1$; en effet, si son degré est plus élevé, on peut la mettre sous la forme

$$Q f(x_1) + R,$$

où R est du degré $n - 1$ au plus, et comme $f(x_1) = 0$, on voit que *toute fonction rationnelle d'une racine d'une équation de degré n peut se mettre sous la forme d'une fonction entière de degré $n - 1$ au plus.*

Si l'on avait une fonction rationnelle de plusieurs racines, on la mettrait d'abord sous la forme

$$A_0 + A_1 x_1 + \ldots + A_{n-1} x^{n-1},$$

où $A_0, A_1, \ldots, A_n$ peuvent contenir $x_2, x_3, \ldots$. Chacun de ces coefficients peut être traité de la même façon par rapport à x_2 et ainsi de suite, et l'on arrive ainsi à une fonction entière des racines, dans laquelle l'exposant d'une racine quelconque ne peut dépasser $n - 1$.

Exemple. — Dans l'équation

$$x^3 + px^2 + qx + r = 0,$$

on peut mettre une fonction d'une racine sous la forme

$$a + bx_1 + cx_1^2,$$

mais il vaut souvent mieux adopter la forme

$$\frac{\alpha x_1 + \beta}{x_1 + \gamma};$$

on l'obtient en remplaçant x par x_1 dans l'identité

$$\begin{aligned} &c^2(x^3+px^2+qx+r)\\ &\quad=(cx^2+bx+a)(cx+pc-b)\\ &\qquad+[qc^2-c(a+bp)+b^2]x+rc^2-apc+ab. \end{aligned}$$

Alors le premier membre étant nul, on a

$$cx_1^2+bx_1+a=-\frac{[qc^2-c(a+bp)+b^2]x_1+rc^2-apc+ab}{cx_1+pc-b}.$$

CHAPITRE III.

SUR L'ÉLIMINATION.

Élimination d'une quantité.

27. Deux équations algébriques entre x et y : l'une du degré m, l'autre de degré n, peuvent être mises sous la forme

$$(1) \qquad f(y) = a_0 y^m + a_1 y^{m-1} + a_2 y^{m-2} + \ldots + a_n = 0,$$

$$(2) \qquad F(y) = b_0 y^n + b_1 y^{n-1} + b_2 y^{n-2} + \ldots + b_n = 0,$$

où a_p et b_p désignent des fonctions de x seul et de degré p. On peut de ces équations en déduire d'autres, satisfaites pour les mêmes valeurs de x et de y.

Pour trouver ces valeurs, on cherche, en général, une équation qui ne contient plus qu'une des inconnues. Cette équation porte le nom d'*équation finale*, et l'on forme cette équation en chassant (en éliminant) l'autre inconnue. Si l'on forme cette équation en x, elle déterminera toutes les valeurs que x peut acquérir, de manière à satisfaire à (1) et (2); en général, à chacune de ces valeurs de x ne correspond qu'une valeur de y, telle que l'ensemble de ces valeurs satisfasse aux équations données : à chaque valeur de x correspond un facteur déterminé du premier degré commun aux deux équations. La question peut donc se présenter sous cet autre point de vue : trouver la condition pour que les polynomes $f(y)$ et $F(y)$ aient un facteur commun. Nous allons faire connaître les méthodes les plus importantes, qui ont pour but de conduire à l'équation finale.

Application de la théorie des fonctions symétriques.

28. L'équation $F(y) = 0$ est de degré n en y et, par suite, elle a n racines fonctions de x; on ne peut pas, en général, les calculer, mais on peut les appeler $y_1, y_2, \ldots, y_n$; à chaque valeur de x cherchée, correspond au moins une valeur, $y_1, y_2, \ldots, y_n$ satisfaisant à $f(y) = 0$; la condition nécessaire et suffisante, pour qu'il existe une valeur de x satisfaisant aux deux équations, est

$$(1) \qquad f(y_1)\, f(y_2) \ldots f(y_n) = 0,$$

car cette équation est satisfaite lorsque l'un des facteurs du premier membre est nul, et seulement dans ce cas. Comme $y_1, y_2, \ldots, y_n$ entrent symétriquement dans l'équation précédente, ils peuvent être éliminés à l'aide de la théorie des fonctions symétriques, en exprimant le premier membre au moyen de $b_0, b_1, \ldots, b_n$, c'est-à-dire en fonction de x seul. L'équation ainsi obtenue ne contient plus que x et est l'équation finale cherchée.

On peut montrer facilement que l'équation finale est, au plus, de degré mn; $f(y)$ est, en effet, homogène du degré m quand on y regarde a_p comme du degré p. Si l'on regarde y_1, y_2, ... comme étant du premier degré, $f(y_1)\, f(y_2) \ldots f(y_n)$ sera homogène et du degré mn. Ainsi, toutes les formules relatives aux fonctions symétriques de $y_1, y_2, \ldots, y_n$ sont homogènes en regardant les racines comme du premier degré et b_p comme du degré p.

L'équation finale en x sera donc du degré mn, si l'on regarde les indices des a et des b comme déterminant les degrés de ces quantités. En réalité, ces indices ne sont égaux qu'à l'exposant de la plus haute puissance de x que peuvent contenir les coefficients. Si donc on considère les degrés par rapport à x, l'homogénéité sera détruite, mais le plus fort exposant de x dans l'équation finale sera mn au plus. b_0 entre en dénominateur dans les coefficients de $F(y)$, mais cela n'a pas d'influence sur le résultat, b_0 ne contenant ni x ni y.

On voit donc que l'*équation finale est, au plus, du degré mn*. Si les équations données sont complètes et générales, c'est-à-dire si tous les termes ont des coefficients tout à fait quelconques et indépendants les uns des autres, le degré sera précisément mn.

Si, en effet, on considère les équations particulières

$$(2) \qquad y = x^m, \qquad x = y^n,$$

on obtient l'équation finale de degré mn

$$(3) \qquad x^{mn} = x,$$

et ce cas doit être contenu dans le cas général, s'il ne s'est pas introduit de solution étrangère; or tel n'est pas le cas; car, soit x_1 une racine de (3), la première équation (2) donne

$$y_1 = x_1^m,$$

et la deuxième équation (2) devient

$$x_1 = x_1^{mn};$$

donc les racines de (3) donnent toutes des solutions de (2); donc il est prouvé que :

Deux équations générales des degrés m et n conduisent à une équation finale du degré mn.

29. Si l'on regarde x et y comme des coordonnées dans un système de coordonnées rectangulaires, les équations données représenteront deux courbes des degrés m et n, et leurs solutions détermineront les intersections des deux courbes. *Deux courbes générales des degrés m et n ont donc mn points communs.* Dans quelques cas particuliers, l'équation finale pourra être de degré moindre. Si l'on part du cas général, et si l'on fait varier les coefficients d'une manière continue pour leur faire prendre des valeurs pour lesquelles le cas particulier se présente, les coefficients des plus hautes puissances de x tendront vers zéro, et autant de racines croî-

tront au delà de toute limite $\left(\text{ce que l'on voit d'ailleurs en changeant } x \text{ en } \frac{1}{x}\right)$. On peut donc dire qu'il y a toujours mn solutions communes ou mn intersections, si l'on compte les solutions qui croissent indéfiniment ou les points qui s'éloignent à l'infini. Ces considérations, qui conservent au théorème relatif aux intersections de deux courbes toute sa généralité, sont d'une grande utilité dans la Géométrie moderne.

Exemple. — Les équations générales du second degré sont

$$f(y) = a_0 y^2 + a_1 y + a_0,$$
$$F(y) = b_0 y^2 + b_1 y + b_0.$$

On trouve, pour le produit $f(y_1) f(y_2)$,

$$a_0^2 y_1^2 y_2^2 + a_0 a_1 y_1 y_2 (y_1 + y_2)$$
$$+ a_1^2 y_1 y_2 + a_0 a_2 (y_1^2 + y_2^2) + a_1 a_2 (y_1 + y_2) + a_2^2$$

où

$$y_1 y_2 = \frac{b_2}{b_0}, \qquad y_1 + y_2 = -\frac{b_1}{b_0}, \qquad y_1^2 + y_2^2 = \left(\frac{b_1}{b_0}\right)^2 - \frac{2 b_2}{b_0}.$$

Voici comment on peut former la fonction $f(y_1) f(y_2) \ldots$. On divise $f(y)$ par $F(y)$, et l'on a, en appelant E un polynome entier,

$$\frac{f(y)}{F(y)} = E + \sum \frac{f(y_i)}{y - y_i} \frac{1}{F'(y_i)}$$

et, par suite, en posant $\frac{f(y)}{F'(y)} = \varphi(y)$,

$$\frac{f(y)}{F(y)} = E + \frac{1}{y} \Sigma \varphi(y_i) + \frac{1}{y^2} \Sigma y_i \varphi(y_i) + \frac{1}{y^3} \Sigma y_i^2 \varphi(y_i) + \ldots,$$

ce qui permet de former $\Sigma \varphi(y_i)$, $\Sigma y_i \varphi(y_i)$, ... par une simple division; on a alors identiquement

$$\begin{vmatrix} \varphi(y_1) & \varphi(y_2) & \ldots & \varphi(y_n) \\ y_1 \varphi(y_1) & y_2 \varphi(y_2) & \ldots & y_n \varphi(y_n) \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ y_1^{n-1} \varphi(y_1) & y_2^{n-1} \varphi(y_2) & \ldots & y_n^{n-1} \varphi(y_n) \end{vmatrix} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ y_1 & y_2 & \ldots & y_n \\ \ldots & \ldots & \ldots & \ldots \\ y_1^{n-1} & y_2^{n-1} & \ldots & y_n^{n-1} \end{vmatrix}$$
$$= \varphi(y_1) \varphi(y_2) \ldots \varphi(y_n) . D^2,$$

en appelant D le second déterminant. D^2 est égal au produit des carrés des différences $(y_i - y_j)$ ou au produit

$$F'(y_1)\,F'(y_2)\ldots F'(y_n);$$

(*voir* nos 25 et 37) cette équation peut s'écrire

$$\begin{vmatrix} \Sigma\,\varphi(y_i) & \Sigma\,y_i\,\varphi(y_i) & \ldots & \Sigma\,y_i^{n-1}\,\varphi(y_i) \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ \Sigma\,y_i^{n-1}\,\varphi(y_i) & \Sigma\,y_i^{n}\,\varphi(y_i) & \ldots & \Sigma\,y_i^{2n-2}\,\varphi(y_i) \end{vmatrix}$$
$$= f(y_1)\,f(y_2)\ldots f(y_n),$$

ce qui fait connaître l'expression de l'équation finale.

Méthode de Labatie.

30. Soient $V_1 = 0$, $V_2 = 0$ les équations données en x et y, ordonnées comme plus haut; soit n le degré de V_2 en y; nous supposerons que V_2 est de degré égal ou inférieur au degré de V_1. Si V_1 et V_2 ont un facteur commun, nous le supprimerons; outre le nombre fini de solutions que nous déterminerons plus bas, les équations seront encore satisfaites pour toutes les valeurs de x et y qui annulent le facteur commun.

Maintenant cherchons le plus grand commun diviseur de V_1 et V_2; on finit par trouver un reste fonction de x seul; en égalant ce reste à zéro, on a l'équation finale, car cette équation exprime que V_1 et V_2 ont un facteur commun. Mais, en examinant les choses de plus près, on voit qu'il peut s'introduire des solutions étrangères, de même qu'il peut en disparaître; cela tient à ce que, pour éviter les fractions, on introduit ou on supprime des facteurs dans les calculs. Ces facteurs sont fonctions de x seul : ceux qui seront introduits dans les dividendes seront désignés par u, ceux qui seront supprimés dans les diviseurs seront désignés par v, les quotients seront désignés par Q. On a alors tout d'abord

$$(1) \qquad u_1 V_1 = Q_1 V_2 + V_3 v_1;$$

on voit alors que les deux systèmes d'équations

$$(2) \qquad \left\{ \begin{aligned} u_1 V_1 &= 0 \\ V_2 &= 0 \end{aligned} \right\} \quad \text{et} \quad \left\{ \begin{aligned} V_2 &= 0, \\ V_3 v_1 &= 0 \end{aligned} \right.$$

ont les mêmes solutions finies, car toutes les valeurs finies qui satisfont à l'un, satisfont à l'autre; si l'un des systèmes a des solutions multiples, l'autre les a aussi et au même degré de multiplicité; car on peut regarder ces systèmes comme des cas limites de systèmes plus généraux sans solutions multiples.

Ce que nous venons de dire n'est vrai que pour les solutions finies; les deux systèmes peuvent ne pas avoir les mêmes solutions infinies; ainsi le système

$$\begin{aligned} x^2+y^2+ax+by+c&=0,\\ x^2+y^2+a_1x+b_1y+c_1&=0 \end{aligned}$$

a deux systèmes de solutions infinies, et l'une de ces équations combinée avec

$$(a-a_1)x+(b-b_1)y+c-c_1=0$$

n'a pas de solutions infinies. Nous laisserons de côté les solutions infinies.

Les systèmes (2) peuvent aussi s'écrire

$$(3)\qquad \left\{\begin{matrix} u_1=0, & V_1=0 \\ V_2=0, & V_2=0 \end{matrix}\right. \quad \text{et} \quad \begin{matrix} v_1=0, & V_2=0, \\ V_2=0, & V_3=0; \end{matrix}$$

nous désignerons ces systèmes par 1, 2, 3, 4.

On voit que, si l'on remplace le système donné 2 par 4, on introduit les solutions étrangères qui appartiennent à 1, et que l'on a éliminé celles qui appartiennent à 3. Dans le cas où u_1 et v_1 ont un facteur commun d_1, on peut l'écarter par la division, car il entre les deux fois en combinaison avec $V_2=0$: il disparaît une fois en divisant par v_1, tandis qu'il s'introduit une autre fois en multipliant par u_1; de la sorte le système donné sera remplacé par

$$(4)\qquad \left\{\begin{matrix} \dfrac{v_1}{d_1}=0 & \text{et} & V_2=0, \\ V_2=0 & & V_3=0; \end{matrix}\right.$$

et les solutions étrangères introduites sont déterminées par

$$(5) \qquad \frac{u_1}{d_1} = 0, \qquad V_2 = 0.$$

On opérera, sur le système $V_2 = 0$, $V_3 = 0$, de la même façon que sur le système primitif, et l'on continuera ainsi de suite jusqu'à ce que l'on parvienne à l'équation finale, en ayant égard aux systèmes mis de côté et à ceux qui déterminent les solutions étrangères. Pour obtenir l'équation finale, il faut la multiplier par $\frac{v_1}{d_1}$ et par les quantités analogues, et la diviser par $\frac{u_1}{d_1}$ et les quantités analogues.

Cependant, s'il s'agit des solutions générales des équations, on doit se rappeler que les racines chassées et introduites jouent un rôle spécial et tout autre que celui des racines, qui sont telles qu'à chacune ne correspond qu'une valeur de y. De cette façon, $\frac{v_1}{d_1} = 0$ doit être combiné avec $V_2 = 0$ et une équation analogue $\frac{v_p}{d_p}$ avec $V_{p+1} = 0$, analogue à $V_2 = 0$. Nous allons maintenant montrer comment on peut simplifier la solution.

31. Nous avons seulement évincé les facteurs communs à un v et à un u de même indice; car on n'a à combiner que dans ce cas u et v avec une même équation. Nous allons toutefois établir le théorème suivant :

Si un u et un v suivant, par exemple u_2 et v_4 ont un facteur commun $x - \alpha$, qui n'appartient pas à un u ou un v intermédiaire, le système $x - \alpha = 0$, $V_3 = 0$ peut être remplacé par $x - \alpha = 0$, $V_5 = 0$.

Considérons, en effet, les équations

$$(6) \qquad \begin{cases} u_2 V_2 = Q_2 V_3 + V_4 v_2, \\ u_3 V_3 = Q_3 V_4 + V_5 v_3, \\ u_4 V_4 = Q_4 V_5 + V_6 v_4. \end{cases}$$

Elles montrent que $x = \alpha$, et les valeurs de y qui satisfont à $u_2 = 0$ et $V_3 = 0$ satisfont aussi à $V_4 = 0$ et $V_5 = 0$ (s'ils

n'annulent pas v_2 ou v_3) et inversement, les valeurs qui satisfont à $v_4 = 0$ et $V_5 = 0$ satisfont aussi à $V_3 = 0$. Il est donc indifférent de combiner les racines communes à $u_2 = 0$ et $v_4 = 0$ avec $V_3 = 0$ ou avec $V_5 = 0$, et ainsi (abstraction faite des solutions infinies) on ne commettra pas de faute en supprimant les facteurs communs à u_2 et v_4. Ainsi, on peut supprimer tout facteur primitivement introduit par une multiplication dans un u, si on le rencontre une première fois dans un v.

Si, par exemple, dans u_2 on trouve le facteur $x - \alpha_1$, et dans u_3 le facteur $x - \alpha_2$, on peut faire disparaître ces facteurs si on les rencontre pour la première fois dans un v, et comme cela a lieu quelque petite que soit la différence entre α_1 et α_2, cela doit encore avoir lieu pour $\alpha_1 = \alpha_2$. Si donc le même facteur a été introduit plusieurs fois, on peut le faire disparaître le même nombre de fois s'il entre dans les v.

On voit maintenant quelles sont les équations à résoudre : d'abord, on a le facteur étranger $\frac{u_1}{d_1}$, et la multiplication suivante donne $\frac{u_1 u_2}{d_1}$; on élimine, par la division, les facteurs contenus dans v_2; en appelant leur produit d_2, il reste à considérer $\frac{u_1 u_2}{d_1 d_2}$, et en multipliant par u_3 et en écartant les facteurs contenus dans v_3, dont on désigne le produit par d_3, on a à considérer $\frac{u_1 u_2 u_3}{d_1 d_2 d_3}$, et ainsi de suite.

Les équations données seront donc remplacées par le système suivant :

$$(7) \quad \begin{cases} \dfrac{v_1}{d_1} = 0, & \dfrac{v_2}{d_2} = 0, & \dfrac{v_3}{d_3} = 0, & \ldots, & \dfrac{v_{n-1}}{d_{n-1}} = 0, \\ V_2 = 0, & V_3 = 0, & V_4 = 0, & \ldots, & V_n = 0, \end{cases}$$

équations qui, abstraction faite des solutions infinies, *ne fourniront que les véritables solutions avec leurs degrés de multiplicité*. Les facteurs étrangers introduits doivent donc, si cela n'a déjà pas été fait dans le courant de l'opération, disparaître de l'équation finale. Le dernier reste est $V_{n+1} v_{n-1}$, et l'on peut supposer $V_{n+1} = 1$, ce reste ne contenant pas y, en

sorte que $v_{n-1} = 0$ est l'équation finale, de laquelle après avoir divisé par α_{n-1} on a écarté toutes les solutions étrangères. Comme, en général, V_n est du premier degré en y, le dernier système fait connaître les solutions qui sont telles qu'à une valeur de x correspond une valeur de y; l'avant-dernier système fait connaître les racines telles qu'à une valeur de x correspondent deux valeurs de y, etc. Comme les solutions multiples ne peuvent se rencontrer que dans des systèmes tout particuliers, on ne trouve que le dernier système, si l'on a affaire à des équations tout à fait générales. En général, l'équation finale, obtenue en annulant le dernier reste de la méthode du plus grand commun diviseur, est de degré trop élevé, puisque l'on doit en ôter les facteurs introduits pour faire les divisions, afin d'éviter les fractions. En opérant sur deux équations du troisième degré, on trouve un reste du onzième degré, et l'on a eu à multiplier deux fois par un polynome du premier ou une fois par un polynome du second degré. La dernière division introduit un facteur du quatrième degré; mais il ne joue aucun rôle, car il n'introduit pas de racines finies.

Si le nombre des racines communes est moindre que celui qui est indiqué par le théorème général, c'est que les racines manquantes sont infinies. En Géométrie, les solutions infinies ont une plus grande importance, et, pour cette raison, nous n'en parlerons plus ici :

Exemple :

$$V_1 = y^3 + 2xy^2 + (2x^2 - 4x)y + x^2 - 4 = 0,$$
$$V_2 = y^2 + 2xy + 2x^2 - 5x + 2 = 0.$$

On supprime dans le premier reste le facteur $x - 2$, et on le combine avec V_2. Le deuxième diviseur est $y + x + 2$; il donne le reste $x^2 - 5x + 6$, et l'on obtient les deux systèmes

$$x = 2, \qquad\qquad x^2 - 5x + 6 = 0,$$
$$y^2 + 2xy + 2x^2 - 5x + 2 = 0, \qquad y + x + 2 = 0,$$

ainsi

$$x = 2, \quad x = 2, \quad x = 2, \quad x = 3,$$
$$y = 0, \quad y = -4, \quad y = -4, \quad y = -5.$$

Comme on devrait obtenir une équation finale du sixième degré, deux valeurs de x sont infinies. Les deux courbes représentées par les équations données ont deux intersections à l'infini et, sur les quatre autres intersections, deux se confondent pour donner un contact.

Méthode d'Euler.

32. Soient

$$(1)\qquad \begin{cases} U = a_0 y^m + a_1 y^{m-1} + a_2 y^{m-2} + \ldots + a_m = 0, \\ V = b_0 y^n + b_1 y^{n-1} + b_2 y^{n-2} + \ldots + b_n = 0, \end{cases}$$

les équations données. Si U et V ont un facteur commun φ de degré p,

$$(2)\qquad \varphi = \alpha_0 y^p + \alpha_1 y^{p-1} + \ldots + \alpha_p,$$

et si l'on pose

$$(3)\qquad \frac{U}{\varphi} = M, \qquad \frac{V}{\varphi} = N,$$

les polynomes NU et MV devront être identiques. N est alors de degré $n-p$ et M de degré $m-p$. Multiplions alors U et V par des polynomes de degrés respectifs, égaux à $n-p$ et $m-p$, et à coefficients indéterminés; et égalons les coefficients des mêmes puissances de y dans les deux produits. Si l'on élimine les coefficients indéterminés entre les équations qui sont du premier degré, on aura les conditions pour que U et V aient un facteur commun de degré p.

Soit

$$(4)\qquad \begin{cases} N = r_0 y^{n-p} + r_1 y^{n-p-1} + \ldots + r_{n-p}, \\ M = t_0 y^{m-p} + t_1 y^{m-p-1} + \ldots + t_{m-p}. \end{cases}$$

On a à sa disposition $m+n-2p$ coefficients indéterminés, et l'identification des deux produits donne $m+n-p$ équations; en éliminant les coefficients indéterminés, on a p équations de condition; si elles sont satisfaites, on a

$$NU = MV.$$

De là, il résulte que les n facteurs de V doivent entrer dans

NU, et que p d'entre eux au moins doivent entrer dans U, puisque N est seulement de degré $n-p$.

Pour $p=1$, on n'a qu'une équation de condition qui est l'équation finale cherchée.

On peut obtenir la forme générale du facteur commun, en remplaçant les polynomes M et N par d'autres M_1 et N_1 de degré moindre, et en annulant les coefficients des puissances supérieures de y dans $N_1U - M_1V$; si l'on pose

$$(5) \qquad N_1U - M_1V = \alpha_0 y^p + \alpha_1 y^{p-1} + \ldots + \alpha_p,$$

le facteur commun à U et V de degré p sera précisément le second membre de (5), si les conditions pour que ce facteur existe sont satisfaites.

Exemple :

$$U = y^3 + a_1 y^2 + a_2 y + a_3 = 0,$$
$$V = y^3 + b_1 y^2 + b_2 y + b_3 = 0;$$

si l'on pose

$$(y^2 + \alpha_1 y + \alpha_2)U = (y^3 + \beta_1 y + \beta_2)V,$$

on a, en identifiant,

$$\begin{aligned} \alpha_1 + a_1 &= \beta_1 + b_1, \\ \alpha_2 + a_1\alpha_1 + a_2 &= \beta_2 + b_1\beta_1 + b_2, \\ a_1\alpha_2 + a_2\alpha_1 + a_3 &= b_1\beta_2 + b_2\beta_1 + b_3, \\ a_2\alpha_2 + a_3\alpha_1 &= b_2\beta_2 + b_3\beta_1, \\ a_3\alpha_2 &= b_3\beta_2. \end{aligned}$$

En éliminant α_1, α_2, β_1, β_2, on a l'équation finale

$$\begin{vmatrix} 1 & 0 & 1 & 0 & a_1 - b_1 \\ a_1 & 1 & b_1 & 1 & a_2 - b_2 \\ a_2 & a_1 & b_2 & b_1 & a_3 - b_3 \\ a_3 & a_2 & b_3 & b_2 & 0 \\ 0 & a_3 & 0 & b_3 & 0 \end{vmatrix} = 0.$$

Pour avoir l'expression du facteur commun, on posera

$$(y + \alpha_1)U - (y + \beta_1)V = my + n;$$

et l'on trouve

$$\alpha_1 + a_1 = \beta_1 + b_1,$$
$$\alpha_1 a_1 + a_2 = \beta_1 b_1 + b_2,$$
$$\alpha_1 a_2 + a_3 = \beta_1 b_2 + b_3 + m,$$
$$\alpha_1 a_3 = \beta_1 b_3 + n;$$

α_1 et β_1 sont donnés par les deux premières équations, et m et n par les deux dernières.

Pour trouver la condition pour qu'il existe un facteur commun du second degré, il suffit de poser $m = n = 0$; alors les conditions sont données en égalant à zéro les déterminants obtenus en prenant trois colonnes dans le Tableau

$$\begin{vmatrix} 1 & a_1 & a_2 & a_3 \\ 1 & b_1 & b_2 & b_3 \\ a_1 - b_1 & a_2 - b_2 & a_3 - b_3 & 0 \end{vmatrix}$$

Ces quatre déterminants, que l'on peut ainsi égaler à zéro, ne fournissent que deux équations distinctes.

Si les équations ainsi obtenues sont satisfaites, on obtient le facteur commun du second degré en éliminant y^3 entre les deux équations données, ce facteur est

$$(a_1 - b_1)y^2 + (a_2 - b_2)y + a_3 - b_3.$$

Méthode de Sylvester.

33. Cette méthode ne diffère pas, au fond, de la précédente. Elle consiste à multiplier les équations données par $y, y^2, y^3, \ldots$ jusqu'à ce que l'on ait obtenu deux équations de degré $m + n - 1$; on a alors $m + n$ équations, entre lesquelles on élimine $y, y^2, y^3, \ldots, y^{m+n-1}$, en les considérant comme des quantités indépendantes entrant au premier degré. On obtient ainsi, en considérant les équations traitées au paragraphe précédent,

$$y^3 + a_1 y^2 + a_2 y + a_3 = 0,$$
$$y^4 + a_1 y^3 + a_2 y^2 + a_3 y = 0,$$
$$y^5 + a_1 y^4 + a_2 y^3 + a_3 y^2 = 0,$$

et

$$y^3 + b_1y^2 + b_2y + b_3 = 0,$$
$$y^4 + b_1y^3 + b_2y^2 + b_3y = 0,$$
$$y^5 + b_1y^4 + b_2y^3 + b_3y^2 = 0,$$

d'où l'équation finale

$$\begin{vmatrix} 0 & 0 & 1 & a_1 & a_2 & a_3 \\ 0 & 1 & a_1 & a_2 & a_3 & 0 \\ 1 & a_1 & a_2 & a_3 & 0 & 0 \\ 0 & 0 & 1 & b_1 & b_2 & b_3 \\ 0 & 1 & b_1 & b_2 & b_3 & 0 \\ 1 & b_1 & b_2 & b_3 & 0 & 0 \end{vmatrix} = 0.$$

Cette équation devient identique à celle que l'on a trouvée tout à l'heure, si l'on échange la troisième ligne avec celle que l'on obtient en retranchant la sixième de la troisième, puis en supprimant la première colonne et la sixième ligne.

Si on laisse de côté la troisième et la sixième équation, on trouve

$$\begin{vmatrix} 0 & 1 & a_1 & a_2 & a_3 \\ 1 & a_1 & a_2 & a_3 & 0 \\ 0 & 1 & b_1 & b_2 & b_3 \\ 1 & b_1 & b_2 & b_3 & 0 \end{vmatrix} = 0;$$

ce qui détermine les deux conditions pour que les équations proposées aient un facteur commun du second degré.

Les résultats des recherches précédentes sur les équations à deux inconnues peuvent se résumer ainsi :

Soient m et n les degrés des deux équations, l'équation finale est de degré mn; dans des cas particuliers ce degré peut s'abaisser, soit parce qu'il existe un facteur commun dans les deux premiers membres des deux équations annulant leur plus grand commun diviseur, soit parce qu'elle présente des racines infinies faisant disparaître les plus hautes puissances de l'inconnue. A chaque racine de l'équation

finale en x correspond, en général, une valeur de y donnée par une équation de la forme

$$Ay + B = 0.$$

Cette équation devient illusoire quand les valeurs de x annulent A et B, y a alors deux valeurs données par une équation de la forme

$$A_1 y^2 + B_1 y + C_1 = 0,$$

si $A_1 = B_1 = C_1 = 0$, y a trois valeurs, etc.

Ces résultats sont surtout mis en lumière dans la méthode de Labatie, parce que toutes les expressions dont on a besoin pour former les équations de condition ou les facteurs sont calculées pendant les opérations; cette méthode est plus commode quand on a affaire à des équations numériques, et doit être alors préférée; tandis que les méthodes d'Euler et de Sylvester, qui donnent le résultat au moyen d'un déterminant, sont préférables dans le cas où le calcul complet des résultats n'est pas exigé.

Méthodes de Bézout et de Laurent.

34. Les méthodes d'élimination que nous avons développées ne sont pas, en réalité, très différentes; elles se réduisent, en définitive, à déduire, des équations données, de nouvelles équations linéaires en y, et à en éliminer les y; la méthode suivante de Laurent a pour but de montrer leurs rapports. Soient $f(y) = 0$ et $\varphi(y) = 0$ les équations données que nous supposerons des degrés m et n ou $m \geq n$. Soient $\theta_1(y)$, $\theta_2(y)$, ..., $\theta_n(y)$ des polynomes de degré $n-1$ linéairement indépendants. En multipliant $f(y)$ par ces polynomes et en divisant les produits par $\varphi(y)$, on obtient n équations de la forme

$$(1) \quad \theta_i(y) f(y) - q_i(y) \varphi(y) = a_i + b_i y + c_i y^2 + \ldots + l_i y^{n-1}.$$

Considérons le déterminant des coefficients des restes

$$R = \Sigma \pm a_1 b_2 c_3 \ldots l_{n-1}.$$

Soient $A_1, A_2, \ldots, A_n$ les mineurs de R relatifs à la première colonne; si nous multiplions les équations (1) respectivement par ces mineurs, et si nous ajoutons, nous obtenons l'équation

$$(2) \qquad f(y)\Sigma A_i\theta_i(y) - \varphi(y)\Sigma A_i q_i(y) = R;$$

cette identité montre que tout facteur commun à $f(y)$ et à $\varphi(y)$ appartient à R; et, comme R ne contient pas y, $R = 0$ est la condition pour que f et φ aient un facteur commun. Si les coefficients de f et de φ dans (2) sont respectivement de degrés $n-1$ et $m-1$, f et φ ont un facteur commun du premier degré, et $R = 0$ est la résultante de $f = 0$ et $\varphi = 0$.

Si R n'est pas nul, (2) donne le théorème suivant :

Si $f(y)$ et $\varphi(y)$ n'ont pas de facteur commun, on peut toujours trouver deux polynomes A *et* B *des degrés $n-1$ et $m-1$, respectivement tels que l'on ait identiquement*

$$A f(y) - B\varphi(y) = 1.$$

Lorsque $R = 0$, on tire des $n-1$ équations distinctes, obtenues en égalant les restes à zéro, les valeurs de $y, y^2, \ldots, y^{n-1}$, où y désigne la racine commune à $f(y) = 0$ et $\varphi(y) = 0$.

On peut remplacer les fonctions θ par des combinaisons linéaires de celles-ci qui soient linéairement indépendantes; les a, les b, ... seront ainsi remplacés par des fonctions linéaires de ces quantités; le déterminant R sera alors multiplié par le déterminant de la substitution correspondante. En faisant varier les coefficients des θ, R acquerra des facteurs divers. Laurent prend les θ égaux à $1, y, y^2, \ldots, y^{n-1}$; dans ce cas, en désignant par $y_1, y_2, \ldots, y_n$ les racines de $\varphi(y) = 0$, les équations (1) deviennent

$$(3) \qquad y_k^i f(y_k) = a_i + b_i y_k + \ldots + l_i y_k^{n-1}.$$

Si l'on forme le déterminant qui a pour élément général le second membre de cette équation, on voit, d'après la forme

de cet élément, qu'il est le produit de R par

$$D = \begin{vmatrix} 1 & y_1 & y_1^2 & \dots & y_1^{n-1} \\ 1 & y_2 & y_2^2 & \dots & y_2^{n-1} \\ \cdot & \cdot\cdot & \cdot\cdot & \dots & \dots\cdot \\ 1 & y_n & y_n^2 & \dots & y_n^{n-1} \end{vmatrix};$$

comme $D = 0$ pour $y_k = y_l$, on voit que D est divisible par le produit des différences des racines y_k, et comme D et ce produit sont de même degré, ils ne peuvent différer que par un facteur numérique, et il est facile de voir que ce facteur est 1 (*voir* p. 48); D^2 est donc le discriminant de $\varphi(y)$. Si, au contraire, on considère le déterminant qui a pour élément général le premier membre de (3), on le trouve égal à

$$f(y_1)\,f(y_2)\dots f(y_n)\,D;$$

on a donc

$$R = f(y_1)\,f(y_2)\dots f(y_n),$$

ce qui (p. 45) donne la forme la plus simple de la résultante.

Maintenant supposons qu'avec ce choix spécial des θ, l'on ait $A_n = 0$: le terme en y^{n-1} dans $\Sigma A_i\theta_i$ s'annule, le coefficient de $f(y)$ est alors de degré $n-2$ dans (1), et $f(y)$ et $\varphi(y)$ ont pour $R = 0$ un facteur commun du second degré; si l'on a encore $A_{n-1} = 0$, ces fonctions ont un facteur commun du troisième degré, et ainsi de suite. Si le facteur commun est de degré $n-1$, il ne devra différer que par des facteurs connus de chaque reste; tous les éléments de R d'une même ligne sont alors proportionnels à ceux d'une autre ligne, et tous les mineurs de R sont nuls.

Laurent évite les divisions à l'aide de certaines fonctions auxiliaires, mais le déterminant qui exprime la résultante est un peu moins simple; comme ces fonctions sont souvent utiles, nous allons les faire connaître.

Soit $F(y) = 0$ une équation de degré m ayant toutes ses racines $a_1, a_2, \dots, a_m$ inégales; on pose

$$\xi_i = \frac{F(y)}{(y-a_i)\,F'(a_i)};$$

les ξ sont des fonctions entières de degré $m-1$, ξ_i se réduit à 1 pour $y=a_i$ et s'annule pour les autres valeurs de a; il en résulte que, si $\psi(y)$ est un polynome quelconque de degré $m-1$ au plus, on a identiquement

$$\psi(y) = \psi(a_1)\xi_1 + \psi(a_2)\xi_2 + \ldots + \psi(a_m)\xi_m.$$

Si l'on prend ψ égal aux m expressions de la forme

$$\frac{f(y)\,\varphi(a_i) - \varphi(y)\,f(a_i)}{y - a_i},$$

on obtient en fonctions linéaires des ξ qui, pour une racine commune de $f(y)=0$, $\varphi(y)=0$, s'annulent à la fois; si l'on élimine les ξ des équations obtenues en égalant les fonctions linéaires à zéro, on obtient la résultante. Laurent montre qu'elle contient en facteur le discriminant de $F(y)$; dans les applications, il n'est pas nécessaire de former ce discriminant; et l'on peut prendre pour les a des nombres arbitraires.

Bézout, Cauchy et Cayley ont fait connaître des méthodes d'élimination qui, au fond, reviennent à prendre (lorsque $m=n$) θ_1, θ_2, ... égaux aux coefficients du quotient de la division de $\varphi(x)$ par $y-x$; q_1, q_2, ... sont alors les coefficients du quotient de la division de $f(x)$ par $y-x$.

Systèmes de plusieurs équations à plus de deux inconnues. Théorème de Bézout.

35. Bézout a démontré, pour la première fois, que l'élimination de $k-1$ quantités entre k équations conduit à une équation finale au plus égale au produit des degrés des équations en question.

Pour plus de simplicité, nous supposerons que les équations données soient au nombre de quatre, nous les supposerons à quatre inconnues x, y, z, u, et tout à fait générales des degrés m, n, p et q; nous supposerons $m \geqq n \geqq p \geqq q$.

De la dernière équation, on tire u^q en fonction entière des autres inconnues et en fonction linéaire des puissances moins élevées de u, et, en multipliant par u, on peut ainsi obtenir toutes les puissances de u en fonction linéaire des puissances

inférieures à q. Si l'on porte ces valeurs dans les autres équations, u n'y entrera plus qu'à la puissance $q-1$ au plus; de même, de l'avant-dernière équation, tirons la valeur de z^p, et, en continuant, on tirera la valeur de y^n de la seconde. Ces substitutions faites, la première équation ne contiendra pas de termes divisibles par y^n, z^p, u^q, elle sera de forme entière et homogène dans le sens où nous avons déjà pris ce mot.

Maintenant multiplions la première équation ordonnée par rapport à y, z, u, et dont les coefficients sont fonctions de x, par un polynome P, contenant tous les termes de la forme $Ay^\beta z^\gamma u^\delta$ non divisibles par y^n, z^p, u^q. Supposons que le premier coefficient de ce polynome soit égal à un. La multiplication une fois effectuée, faisons encore disparaître les termes divisibles par y^n, z^p, u^q, l'équation contiendra autant des autres termes indéterminés que de coefficients indéterminés, et cela sous forme linéaire; on peut les déterminer de manière à annuler tous les termes en y, z, u et le résultat est alors l'équation finale.

Pour déterminer le degré de l'équation finale, nous observerons que le degré de la première équation est m. Le degré du facteur par lequel on l'a multipliée, et qui, au moyen d'indices convenablement choisies, est rendu homogène, étant μ, le produit sera de degré $m+\mu$, le nombre des termes du produit est npq, c'est le nombre des termes du produit

$$(1+y+y^2+\ldots+y^{n-1})(1+z+\ldots+z^{p-1})(1+u+\ldots+u^{q-1}),$$

qui ne diffère du premier que par ses coefficients qui sont linéaires par rapport aux coefficients indéterminés. Soient $l^{(r)}$ un terme de P et $\alpha^{(r)}$ son coefficient; $\alpha^{(r)}l^{(r)}$ est de degré μ, il se trouve multiplié dans le produit par un facteur de degré m en x. Le produit a la forme

$$(a\alpha^{(0)}+b\alpha^{(1)}+\ldots)l^{(0)}+(d\alpha^{(0)}+c\alpha^{(1)}+\ldots)l^{(1)}+\ldots;$$

si l'on égale à zéro les coefficients de $l^{(0)}$, $l^{(1)}$, ..., et si, entre les équations obtenues, on élimine $\alpha^{(0)}$, $\alpha^{(1)}$, ..., ce qui se fera en égalant à zéro un certain déterminant, les termes de la diagonale sont les coefficients de termes de la forme

$\alpha^{(r)} l^{(r)}$. Ces coefficients sont de degré m, et leur produit est de degré $mnpq$. Tous les termes de l'équation finale ont donc une somme d'indices égale à $mnpq$, et, par rapport à x, elle sera de degré $mnpq$ au plus. Il est facile de voir que ce degré n'est pas, en général, inférieur à $mnpq$; en effet, si l'on considère les équations particulières

$$x = y^m, \qquad y = z^n, \qquad z = u^p, \qquad u = x^q,$$

leur équation finale est bien de degré $mnpq$.

36. Si l'on n'introduit que $npq - 2$ coefficients indéterminés dans P, on peut faire disparaître tous les termes, à l'exception de celui qui contient seulement x et de celui qui contient une des autres inconnues au premier degré; on a alors une équation qui détermine cette inconnue lorsque l'on a tiré x de l'équation finale, et la discussion s'achève comme dans la méthode d'Euler exposée à propos de deux équations; cette méthode d'Euler, en réalité, est identique à celle de Bézout.

Exemple :

$$x^2 + yz = a^2, \qquad y^2 + xz = b^2, \qquad z^2 + xy = c^2,$$

on a

$$\begin{aligned} y^2 &= b^2 - xz, \\ z^2 &= c^2 - xy, \\ y^2 z &= b^2 x - xc^2 + x^2 y, \\ yz^2 &= c^2 y - xb^2 + x^2 z, \\ y^2 z^2 &= b^2 c^2 - b^2 xy - c^2 xz + x^2 yz \end{aligned}$$

et

$$(yz + \alpha_1 z + \beta_1 y + \gamma_2)(yz + x^2 - a^2) = 0.$$

Si l'on effectue la multiplication et si l'on remplace y^2, z^2, $y^2 z$, yz^2 par leurs valeurs, on obtient, en égalant les coefficients de yz, z, y et le terme indépendant à zéro, et en éliminant les coefficients α_1, β_1, γ_2, l'équation finale

$$\begin{vmatrix} 2x^2 - a^2 & 0 & 0 & 1 \\ -c^2 x & 2x^2 - a^2 & b^2 & 0 \\ -b^2 x & c^2 & 2x^2 - a^2 & 0 \\ b^2 c^2 & -b^2 x & -c^2 x & x^2 - a^2 \end{vmatrix} = 0.$$

On voit que tous les termes d'une ligne diagonale sont du second degré, ce qui confirme ce que nous avons dit sur le degré de ces termes en général. Pour trouver y et z, posons

$$(z+\alpha_0 y+\alpha_1)(yz+x^2-a^2)=0$$

ou

$$z^2y+\alpha_0 y^2 z+\alpha_1 yz+z(x^2-a^2)+\alpha_0 y(x^2-a^2)+\alpha_1(x^2-a^2)=0;$$

si l'on remplace z^2y et y^2z par leurs valeurs, et si l'on égale à zéro le coefficient de yz, on a

$$z(2x^2-a^2+\alpha_0 b^2)+y[\alpha_0(2x^2-a^2)+c^2]-x(b^2+\alpha_0 c^2)=0:$$

en égalant à zéro les coefficients de y ou de z, on a

$$y[b^2c^2-(2x^2-a^2)^2]=x[b^4-c^2(2x^2-a^2)],$$
$$z[b^2c^2-(2x^2-a^2)^2]=x[c^4-b^2(2x^2-a^2)].$$

Les équations que nous venons de traiter peuvent être résolues plus simplement, en ajoutant les deux dernières et en les multipliant entre elles, puis en éliminant $y+z$ et yz. L'équation finale du huitième degré se ramène au quatrième, en posant $x^2=u$.

37. Nous pouvons donner à la méthode que nous venons d'exposer une autre forme; elle revient, en réalité, à retrancher d'abord de l'une des équations les autres, multipliées par des polynomes déterminés. Par exemple, pour faire disparaître de $f=0$ de degré $n>p$ les termes qui contiennent x^p, x^{p+1}, ..., x^n, au moyen de l'équation

$$\varphi=x^p+a_1x^{p-1}+\ldots=0,$$

on a

$$x^p\quad=\varphi+\ldots,$$
$$x^{p+1}=x\varphi-a_1x^p+\ldots=(x-a_1)\varphi+\ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$x^n\quad=A_{n-p}\varphi+\ldots,$$

où A_{n-p} est de degré $n-p$, en sorte que, pour faire disparaître les termes en x^p, x^{p+1}, ..., on écrit

$$f-B_{n-p}\varphi=\ldots,$$

où B_{n-p} est un polynome de degré $n-p$.

De cette façon si $\varphi_1 = 0$, $\varphi_2 = 0$, $\varphi_3 = 0$, $\varphi_4 = 0$ sont les équations considérées au n° 35, nous avons d'abord formé l'équation

$$\varphi_1 + A\varphi_2 + B\varphi_3 + C\varphi_4 = 0;$$

nous avons ensuite multiplié cette équation par un facteur, et nous avons combiné le résultat de la même façon avec les trois équations $\varphi_2 = 0$, $\varphi_3 = 0$, $\varphi_4 = 0$; nous avons alors trouvé

$$\lambda_1\varphi_1 + (\lambda_1 A + A_1)\varphi_2 + (\lambda_1 B + B_1)\varphi_3 + (\lambda_1 C + C_1)\varphi_4 = 0:$$

et cette équation, quand on y suppose les coefficients du polynome multiplicateur convenablement choisis, est la résultante; en sorte que celle-ci est de la forme

$$\lambda_1\varphi_1 + \lambda_2\varphi_2 + \lambda_3\varphi_3 + \lambda_4\varphi_4 = R = 0.$$

Théorème de Jacobi.

38. Pour simplifier, nous ne considérerons, dans ce qui va suivre, que deux équations; néanmoins, nos conclusions seront tout à fait générales, et nos raisonnements pourront sans difficulté s'étendre à un plus grand nombre d'équations.

Soient les trois équations

$$\varphi_1(x, y, z) = 0, \qquad \varphi_2(x, y, z) = 0, \qquad \varphi_3(x, y, z) = 0;$$

pour la commodité du langage, nous supposerons que ces trois équations soient celles de trois surfaces. Alors les coordonnées de leurs intersections sont les solutions de ces équations. Soient m, n, p respectivement les degrés des équations en question, posons $mnp = \mu$; nous désignerons par $(x_i y_i z_i)$ les coordonnées des intersections et nous supposerons $i = 1, 2, \ldots, \mu$.

Il existe un théorème important sur les fonctions symétriques des coordonnées des points d'intersection des trois surfaces, dû à Jacobi et que nous allons démontrer.

Soit $f(x) = 0$, une équation ayant toutes ses racines x_1, x_2, ..., x_n distinctes; en désignant par $\varphi(x)$ un polynome

quelconque, la formule relative à la décomposition en éléments simples donne

$$\frac{x\varphi(x)}{f(x)} = a_0 x^p + a_1 x^{p-1} \ldots + k + \sum \frac{x_i \varphi(x_i)}{(x - x_i) f'(x_i)},$$

formule d'où les termes entiers disparaissent si le degré de $\varphi(x)$ est inférieur à $n-1$. Si l'on y fait $x = 0$, on a

$$k = \sum \frac{\varphi(x_i)}{f'(x_i)},$$

et $k = 0$ si le degré de φ est inférieur à $n-1$.

Posons maintenant

$$(1) \qquad \begin{cases} \lambda_{11}\varphi_1 + \lambda_{12}\varphi_2 + \lambda_{13}\varphi_3 = X, \\ \lambda_{21}\varphi_1 + \lambda_{22}\varphi_2 + \lambda_{23}\varphi_3 = Y, \\ \lambda_{31}\varphi_1 + \lambda_{32}\varphi_2 + \lambda_{33}\varphi_3 = Z; \end{cases}$$

X, Y, Z ne contenant respectivement que x, que y et que z, ces quantités sont de degré μ; nous supposerons nos équations générales, en sorte que le déterminant fonctionnel

$$D = \begin{vmatrix} \frac{\partial\varphi_1}{\partial x} & \frac{\partial\varphi_1}{\partial y} & \frac{\partial\varphi_1}{\partial z} \\ \frac{\partial\varphi_2}{\partial x} & \frac{\partial\varphi_2}{\partial y} & \frac{\partial\varphi_2}{\partial z} \\ \frac{\partial\varphi_3}{\partial x} & \frac{\partial\varphi_3}{\partial y} & \frac{\partial\varphi_3}{\partial z} \end{vmatrix}$$

sera différent de zéro aux points d'intersection de nos trois surfaces. Nous poserons

$$\Delta = \Sigma \pm \lambda_{11}\lambda_{22}\lambda_{33},$$

Δ sera le déterminant des équations (1), et nous aurons

$$\Delta\varphi_i = A_i X + B_i Y + C_i Z.$$

Nous pouvons combiner les μ racines des équations $X = 0$, $Y = 0$, $Z = 0$ ensemble de μ^3 manières; ces combinaisons comprendront les coordonnées simultanées des μ intersec-

tions de nos surfaces. Chacune de ces μ^3 combinaisons annule $\Delta\varphi_i$ et, comme les φ s'annulent à la fois et aux points d'intersection seulement, Δ devra s'annuler pour les autres combinaisons en nombre $\mu^3 - \mu$.

Le théorème de Jacobi apprend à évaluer la fonction symétrique

$$\sum \frac{\psi(x, y, z)}{D},$$

où ψ est une fonction entière quelconque, et où la sommation s'étend à tous les points d'intersection des trois surfaces. Si nous différentions les équations (1), en négligeant les termes nuls avec les φ, nous aurons

$$(2)\quad \begin{cases} \lambda_{11}\dfrac{\partial\varphi_1}{\partial x} + \lambda_{12}\dfrac{\partial\varphi_2}{\partial x} + \lambda_{13}\dfrac{\partial\varphi_3}{\partial x} = X', \\ \lambda_{11}\dfrac{\partial\varphi_1}{\partial y} + \lambda_{12}\dfrac{\partial\varphi_2}{\partial y} + \lambda_{13}\dfrac{\partial\varphi_3}{\partial y} = 0, \\ \lambda_{11}\dfrac{\partial\varphi_1}{\partial z} + \lambda_{12}\dfrac{\partial\varphi_2}{\partial z} + \lambda_{13}\dfrac{\partial\varphi_3}{\partial z} = 0, \end{cases}$$

et deux systèmes analogues. Formons le déterminant

$$X'Y'Z' = \begin{vmatrix} X' & 0 & 0 \\ 0 & Y' & 0 \\ 0 & 0 & Z' \end{vmatrix}$$

et remplaçons ses éléments par leurs valeurs (2), nous obtenons le produit des deux dé erminants D et Δ, donc

$$D\Delta = X'Y'Z'.$$

La somme que nous avons voulu évaluer se réduit alors à

$$\sum \frac{\psi\Delta}{X'Y'Z'};$$

elle doit s'étendre à toutes les intersections; mais on peut, sans inconvénient, l'étendre à toutes les combinaisons des racines de $X = 0$, $Y = 0$, $Z = 0$, à cause de la présence du facteur Δ, nul pour les combinaisons qui n'appartiennent pas

aux intersections. Cette somme se décompose en d'autres de la forme

$$\sum \frac{x^\alpha y^\beta z^\gamma}{X'Y'Z'} = \sum \frac{x^\alpha}{X'} \sum \frac{y^\beta}{Y'} \sum \frac{z^\gamma}{Z'}.$$

Ce produit, d'après ce que nous avons vu, s'annule quand α, β, γ ne sont pas simultanément égaux ou supérieurs à $\mu - 1$. Si le degré de $\psi\Delta$ est alors inférieur à $3(\mu - 1)$, la somme en question sera nulle; si le degré $\psi\Delta$ est égal à $3(\mu - 1)$, elle sera égale au rapport des coefficients de $x^{\mu-1}$, $y^{\mu-1}$, $z^{\mu-1}$ au numérateur et au dénominateur.

Comme la différence des degrés du numérateur et du dénominateur n'est pas altérée par l'introduction du facteur Δ, on peut dire que la somme en question est nulle quand le degré de ψ est moindre que le degré de D.

Méthode de Poisson.

37. Considérons d'abord trois équations des degrés m, n, p

(1) $\varphi_m(x, y, z) = 0, \qquad \varphi_n(x, y, z) = 0, \qquad \varphi_p(x, y, z) = 0.$

Éliminons z entre les deux dernières, nous aurons

(2) $$z = \frac{\psi_1(x, y)}{\psi_2(x, y)}; \qquad \psi(x, y) = 0.$$

La dernière équation est de degré np, et ψ_1, ψ_2 sont des fonctions entières. Si donc on regarde x comme une quantité connue, on aura np valeurs de y et np valeurs correspondantes de z. Nous supposerons les équations données homogènes dans le sens déjà donné à ce mot, c'est-à-dire que nous supposerons, par exemple, à $y^r z^s$ un coefficient d'indice $m - r - s$ dans la première équation, et ce coefficient sera une fonction entière de x dont le degré sera égal à son indice. Nos deux équations (2) sont alors homogènes dans le sens convenu.

Nous appellerons fonctions symétriques des np solutions (y_1, z_1), (y_2, z_2), ... des fonctions qui ne changent pas quand

on permute à la fois z_p et z_q, y_p et y_q. Les fonctions symétriques des solutions seront des fonctions symétriques de $y_1, y_2, \ldots$ si l'on y remplace $z_1, z_2, \ldots$ en faisant usage de la première formule (2), et pourront être exprimées rationnellement à l'aide des coefficients de la seconde équation (2), coefficients qui sont fonctions de x. Comme les équations dont on a fait usage sont homogènes, les fonctions symétriques homogènes par rapport aux solutions seront homogènes par rapport aux coefficients. Par exemple

$$y_1 z_1 + y_2 z_2 + \ldots + y_{np} z_{np}$$

sera transformé en

$$y_1 \frac{\psi_1(x, y_1)}{\psi_2(x, y_1)} + y_2 \frac{\psi_1(x, y_2)}{\psi_2(x, y_2)} + \ldots,$$

et sera exprimable en fonction de x seul, c'est-à-dire en fonction des coefficients des équations données. Comme nos fonctions symétriques sont fractionnaires, on doit s'attendre à ce que leur expression sera fractionnaire et que la différence entre le degré des numérateurs et du dénominateur sera le degré de la fonction symétrique. Nous allons prouver que le résultat est entier et que le dénominateur divise exactement le numérateur. En effet, s'il n'en était pas ainsi, il existerait des valeurs finies de x rendant infinies des fonctions symétriques entières de $y_1, z_1, y_2, z_2, \ldots$, ce qui ne peut arriver que si l'une des quantités $y_1, z_1, y_2, z_2, \ldots$ est infinie. Or, les équations $\psi_n = 0$, $\psi_p = 0$ sont tout à fait générales, même quand x prend une valeur particulière, et l'on sait que de pareilles équations n'ont pas de solutions infinies.

La condition pour que la première équation soit satisfaite par un des systèmes trouvés est

$$(3) \qquad \varphi_m(x, y_1, z_1)\,\varphi_m(x, y_2, z_2)\ldots\varphi_m(x, y_{np}, z_{np}) = 0;$$

ce produit est une fonction symétrique entière de x_1, y_1, x_2, y_2, ... et peut s'exprimer en fonction de x; chaque facteur est une fonction homogène de degré m, et ce degré ne

change pas quand on passe des fonctions symétriques aux coefficients; l'équation finale est donc de degré mnp.

38. Si l'on élimine z entre $\varphi_m = 0$ et $\varphi_n = 0$, on obtient une équation entre x et y de degré mn; si l'on élimine z entre $\varphi_n = 0$ et $\varphi_p = 0$, on obtient une équation de degré np. En éliminant y entre ces deux dernières équations, on obtient une équation de degré mn^2p, rationnelle en x. *On ne peut donc employer ce procédé d'élimination sans introduire de solutions étrangères*; mais on peut utiliser ces calculs pour obtenir y puis z rationnellement en fonction de x.

Il est facile d'interpréter les solutions étrangères, si l'on considère les deux équations en x et y : la première exprime que φ_m et φ_n ont un facteur commun; la seconde exprime que φ_n et φ_p ont un facteur commun. L'équation obtenue par notre dernier procédé exprime donc que la première et la deuxième équation ont une solution commune, que la deuxième et la troisième ont une solution commune, tandis qu'il faudrait exprimer que les trois équations ont une solution commune.

Si l'on désigne par

$$z_1, z_2, \ldots, z_m; \quad z'_1, z'_2, \ldots, z'_n; \quad z''_1, z''_2, \ldots, z''_p$$

les valeurs de z tirées des trois équations, on peut combiner, pour les égaler, une valeur de chaque groupe, ce qui peut se faire de mnp manières, tandis que l'on peut obtenir mn^2p combinaisons en égalant une valeur du premier groupe avec une valeur du deuxième, et une du deuxième avec une du troisième.

Si l'on considère, par exemple, trois équations représentant trois surfaces du second ordre, en éliminant deux fois z, on obtient les équations des courbes du quatrième ordre qui projettent l'intersection de deux surfaces sur le plan des xy ; ces courbes se coupent en 16 points; 8 de ces points sont les projections des intersections des trois surfaces; les 8 autres sont les projections de points d'intersections de parallèles à l'axe des z, avec les courbes, intersections qui sont distinctes.

39. Nous avons montré que, dans un système de trois équations de degrés m, n, p, deux inconnues pouvaient s'exprimer rationnellement au moyen de la troisième, cette dernière étant déterminée par une équation de degré mnp. Nous avons montré que, si les équations étaient tout à fait générales, ce degré était précisément mnp. Dans des cas particuliers, le degré peut s'abaisser; alors une ou plusieurs solutions sont infinies. De même, les valeurs de y et z exprimées en x pourraient être indéterminées; ce cas se présenterait, comme on l'a vu, à propos de deux équations, si, à une valeur de x, correspondaient plusieurs valeurs de y et z, données alors par des équations de degré supérieur.

On voit facilement que la démonstration que nous venons de donner s'étendrait à quatre équations à quatre inconnues, et nous n'entrerons pas, à ce sujet, dans de plus amples développements.

40. La méthode que nous venons de donner pour le calcul des fonctions symétriques est très pénible et peut être simplifiée comme il suit : écrivons la première équation donnée ainsi

$$a_m - u = 0,$$

a_m désignant les termes qui ne contiennent que x, et $-u$ désignant les autres termes; si, comme plus haut, on remplace y_1, z_1, y_2, z_2, ... par leurs valeurs (3), u prend np valeurs u_1, u_2, ..., et l'équation finale est

$$(4) \qquad (a_m - u_1)(a_m - u_2)\ldots(a_m - u_{np}) = 0;$$

on exprime alors z rationnellement en fonction de x et y [37 (2)], et si l'on porte ces valeurs dans u, on a

$$(5) \qquad u = \varphi(x, y).$$

Si l'on élimine y entre cette équation et

$$\psi(x, y) = 0.$$

on obtient une équation en u de degré np; et quoique u se

présente sous forme fractionnaire, on voit, comme plus haut, que les coefficients de l'équation en u sont des fonctions entières de x. Comme l'équation en u peut s'écrire

$$(u - u_1)(u - u_2)\ldots(u - u_{np}) = 0,$$

il suffit d'y remplacer u par a_m pour obtenir l'équation finale.

On pourrait aussi bien tout de suite remplacer u par a_m dans (5), ce qui revient à éliminer y de l'équation $\psi = 0$ et de la première après en avoir fait disparaître z. Mais la forme du résultat serait changée, et l'on ne verrait pas immédiatement le facteur que l'on doit supprimer, tandis que l'on sait que, quand on a u, c'est le coefficient de u^{np}.

Exemple. — De

$$x^2 + yz = a^2,$$
$$y^2 + zx = b^2,$$
$$z^2 + xy = c^2$$

on tire

$$z = \frac{b^2 - y^2}{x}; \qquad y^4 - 2b^2y^2 + x^3y - c^2x^2 + b^4 = 0;$$

$$yz = u = \frac{b^2y - y^3}{x}; \qquad y^3 - b^2y + ux = 0;$$

éliminons y entre les deux équations en y, le coefficient de u^4 sera supprimé et, à la place de u, on mettra $a^2 - x^2$; on retrouve ainsi l'équation en x du huitième degré trouvée page 62.

CHAPITRE IV.

TRANSFORMATION DES ÉQUATIONS.

Transformations linéaires.

41. Étant donnée une équation, on peut en déduire d'autres dont les racines sont liées aux racines de la proposée par des relations données.

Étant donnée l'équation

$$(1) \qquad f(x) = 0,$$

on peut former une équation

$$(2) \qquad \varphi(u) = 0$$

telle qu'entre les racines x et u de ces équations il existe la relation

$$(3) \qquad x = \frac{a + bu}{c + du} \qquad \text{ou} \qquad u = \frac{a - cx}{dx - b},$$

où a, b, c, d sont indépendants de u et de x.

Pour obtenir l'équation (2), il suffit de remplacer dans (1) x par sa valeur (3); on obtient ainsi l'équation

$$(4) \qquad f\left(\frac{a + bu}{c + du}\right) = 0$$

qui, après l'évanouissement des dénominateurs, se ramène à la forme ordinaire.

Pour résoudre l'équation (1), on peut résoudre l'équation $\varphi(u) = 0$ et remplacer, dans l'expression de x en fonction de u, u par sa valeur; les équations (1) et (2) sont donc de

même degré et chaque racine de l'une fournit une racine de l'autre. Si l'une des équations est irréductible, l'autre l'est aussi; en effet, si l'une d'elles était réductible, elle se décomposerait en d'autres plus simples que l'on pourrait transformer individuellement, et l'autre équation serait elle-même décomposable.

On peut effectuer la transformation en posant successivement

$$x = \frac{b}{d} + u_1; \qquad u_1 = \frac{ad - bc}{d^2 u_2}; \qquad u_2 = \frac{c}{d} + u,$$

de sorte que les transformations linéaires se ramènent aux trois types

$$x = \alpha u; \qquad x = u + h; \qquad x = \frac{1}{u}.$$

42. La substitution $x = \alpha u$ fournit une équation dont les racines sont avec celles de la proposée dans un rapport fixe. Si l'équation proposée a des coefficients fractionnaires (le coefficient de la plus haute puissance de l'inconnue étant réduit à l'unité), on peut toujours disposer de α de telle sorte que l'équation transformée ait tous ses coefficients entiers. Si l'on a, par exemple,

$$f(x) = x^n + \frac{a_1}{b_1} x^{n-1} + \frac{a_2}{b_2} x^{n-2} + \ldots + \frac{c_n}{b_n} = 0.$$

Si l'on pose $x = \frac{u}{\alpha}$, et si l'on multiplie par α^n, on a

$$\varphi(u) = u^n + \frac{a_1}{b_1} \alpha u^{n-1} + \frac{a_2}{b_2} \alpha^2 u^{n-2} + \ldots + \frac{a_n}{b_n} \alpha^n = 0;$$

pour que $\frac{a_1}{b_1}\alpha$, $\frac{a_2}{b_2}\alpha^2$, ..., $\frac{a_n}{b_n}\alpha^n$ perdent leur forme fractionnaire si toutes les fractions $\frac{a_1}{b_1}$, $\frac{a_2}{b_2}$, $\cdots$ sont irréductibles, il faut que α contienne les facteurs premiers ou littéraux qui entrent dans b_1, b_2, ..., b_n. Pour trouver l'exposant q avec lequel un facteur β doit entrer dans α, on observera que β^{pq} entrera en facteur dans α^p; si donc, dans le dénominateur b_p,

il entre le facteur β^r, il disparaîtra si $pq \geqq r$ ou si $q \geqq \frac{r}{p}$. On divisera donc les exposants des facteurs qui entrent dans les dénominateurs par l'indice du terme correspondant et l'on prendra pour exposant q de β le plus petit entier tel que $q \geqq \frac{r}{p}$.

Exemple :

$$x^4 + \frac{1}{ab}x^3 + \frac{1}{a^2 b}x^2 + \frac{1}{a^4 b^2}x + \frac{1}{a^3 b^3} = 0;$$

les exposants de a dans les dénominateurs sont

$$1,\ 2,\ 4,\ 3,$$

en les divisant par 1, 2, 3, 4, on a

$$1 \quad 1 \quad \tfrac{4}{3} \quad \tfrac{3}{4};$$

la valeur entière minima plus grande que toutes ces quantités est 2; un calcul analogue pour b donne

$$\begin{matrix} 1 & 1 & 2 & 3 \\ 1 & \tfrac{1}{2} & \tfrac{2}{3} & \tfrac{3}{4}; \end{matrix}$$

on a ainsi

$$x = \frac{u}{a^2 b},$$

et l'équation transformée devient

$$u^4 + au^3 + a^2 bu^2 + a^2 bu + a^5 b = 0;$$

si l'on prend $\alpha = -1$, ou $x = -u$, on obtient une équation dont les racines sont égales à celles de la proposée changées de signe.

43. La substitution

$$x = u + h$$

peut servir, en choisissant convenablement h, à faire disparaître un terme de l'équation. La formule de Taylor, en l'appliquant à

$$(5) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1}x + a_n = 0,$$

donne, en effet,

$$(6)\quad \begin{cases} f(h+u) = f(h) + f'(h)\frac{u}{1} + f''(h)\frac{u^2}{1.2} + \dots \\ \qquad + f^{n-1}(h)\frac{u^{n-1}}{(n-1)!} + f^n(h)\frac{u^n}{n!}; \end{cases}$$

le coefficient de u^n est 1, car $f^n(h) = n!$; le coefficient de u^{n-1} est $a_1 + nh$; on le fera disparaître en prenant

$$h = -\frac{a_1}{n}.$$

Le coefficient de u^{n-2} est

$$a_2 + (n-1)a_1 h + \tfrac{1}{2}n(n-1)h^2;$$

et on pourra le faire disparaître de deux manières par des choix convenables de h. En général, le coefficient de u^{n-p} pourra s'annuler pour p valeurs de h qui sont racines d'une équation de degré p. Si l'on veut annuler le dernier terme, il faudra résoudre une équation du degré n, qui, au nom de l'inconnue près, sera identique à la proposée, ce qui s'explique en observant que faire disparaître le dernier terme, c'est exprimer que l'équation transformée a une racine nulle, ce qui revient à trouver les valeurs de h qui, soustraites des racines de la proposée, donnent une différence nulle. Les valeurs de h en question sont donc les racines de la proposée.

Exemple :

$$x^3 + Ax^2 + Bx + C = 0$$

se ramène à la forme

$$u^3 + au + b = 0$$

en posant

$$x = u - \frac{A}{3};$$

alors

$$a = B - \frac{A^2}{3}, \qquad b = C - \frac{1}{3}AB + \frac{2}{27}A^3$$

44. En combinant les deux substitutions dont il vient d'être question, on obtient la suivante :

$$x = \alpha u + h.$$

Nous examinerons le cas particulier

(7) $$x = h - u.$$

Il peut arriver que l'équation en u, abstraction faite du nom de l'inconnue, soit identique à l'équation proposée : si x_1 est alors une des racines de cette dernière, $h - x_1$ en sera une autre ; appelons-la x_2 ; alors

(8) $$x_1 + x_2 = h;$$

comme x_1 est une racine arbitraire, l'équation jouira de cette propriété que les racines ont deux à deux pour somme h, et, si l'équation est de degré impair, une racine sera égale à $\frac{h}{2}$, et le facteur $x - \frac{h}{2}$ peut être éliminé par la division ; nous supposerons alors l'équation de degré pair.

Une telle équation peut être résolue à l'aide d'une équation de degré moitié moindre et d'équations du second degré. En effet, si l'on pose

(9) $$y = x(h - x) \quad \text{ou} \quad x^2 - hx + y = 0$$

dans l'équation donnée (5), y n'aura que $\frac{n}{2}$ valeurs ; car

$$y_1 = x_1(h - x_1) \quad \text{et} \quad y_2 = x_2(h - x_2)$$

sont égaux en vertu de la relation $x_1 + x_2 = h$.

Les fonctions symétriques des y seront aussi des fonctions symétriques des x ; cette considération permet de former l'équation en y ; mais on peut aussi l'obtenir en éliminant x entre (5) et (9).

Si l'on peut résoudre l'équation en y, $f(x)$ pourra se décomposer en $\frac{n}{2}$ facteurs du second degré comme il suit :

$$f(x) = (x^2 - hx + y_1)(x^2 - hx + y_2)\ldots\left(x^2 - hx + y_{\frac{n}{2}}\right).$$

On voit, en comparant cette valeur de $f(x)$ avec (5) que

$$2a_1 = -nh.$$

Si l'on veut vérifier qu'une équation jouit de la propriété en question, il n'y a qu'à voir si elle est inaltérée quand on change x en $-\frac{2a_1}{n} - x$.

Exemple :

$$x^6 - 9x^5 + 30x^4 - 45x^3 + 25x^2 + 6x + 4 = 0.$$

Cette équation ne change pas quand on remplace x par $3 - x$; si l'on élimine x à l'aide de la relation

$$x^2 - 3x + y = 0,$$

on trouve

$$y^3 - 3y^2 - 2y + 4 = 0,$$

qui se décompose en

$$y - 1 = 0 \qquad \text{et} \qquad y^2 - 2y - 4 = 0.$$

Équations réciproques.

45. Si, dans une équation dans laquelle x est l'inconnue, on fait la substitution

$$(1) \qquad x = \frac{1}{u},$$

on obtient une nouvelle équation dont les racines sont les inverses des racines de la proposée. Si l'on tombe sur une équation identique avec la proposée, celle-ci a ses racines deux à deux inverses l'une de l'autre; si elle est de degré pair et si elle est de degré impair, une racine devra être égale à ± 1. Dans ce dernier cas, on supposera que l'on ait écarté le facteur $x \mp 1$ par la division; alors l'équation peut être résolue au moyen d'une équation de degré moitié moindre et d'équations du second degré.

En effet, si l'on pose

$$(2) \qquad y = x + \frac{1}{x} \qquad \text{ou} \qquad x^2 - xy + 1 = 0,$$

les valeurs de y

$$y_1 = x_1 + \frac{1}{x_1}, \qquad \text{et} \qquad y_2 = x_2 + \frac{1}{x_2}$$

seront égales si $x_1 x_2 = 1$; y a donc moitié moins de valeurs que x. On obtient l'équation en y, en éliminant x entre la proposée et (2).

La condition pour qu'une équation soit réciproque est qu'elle reste inaltérée quand on y change x en $\frac{1}{x}$; dans le cas où l'équation est de degré pair, il faut que la suite des coefficients soit symétrique (le premier doit être égal au dernier, le second à l'avant-dernier, etc.). Si l'équation est de degré impair, la suite des coefficients doit être symétrique si l'on peut diviser le premier membre par $x+1$; si le premier membre peut être divisé par $x-1$, la suite des coefficients doit être symétrique, à cela près que les coefficients numériquement égaux doivent avoir des signes contraires. La forme générale des équations réciproques de degré pair est donc

$$(3) \quad x^{2n} + 1 + a_1(x^{2n-1} + x) + a_2(x^{2n-2} + x^2) + \ldots + a_n x^n = 0.$$

La réduction peut s'obtenir de la manière suivante : on divise par x^n et l'on a

$$(4) \quad x^n + \frac{1}{x^n} + a_1\left(x^{n-2} + \frac{1}{x^{n-1}}\right) + a_2\left(x^{n-1} + \frac{1}{x^{n-2}}\right) + \ldots + a_n = 0;$$

on pose

$$(5) \qquad x + \frac{1}{x} = y,$$

d'où

$$x^2 + \frac{1}{x^2} = y^2 - 2,$$

et, en multipliant membre à membre ces deux formules,

$$x^3 + \frac{1}{x^3} = y^3 - 3y.$$

En général, si l'on fait

(6) $$x^p + \frac{1}{x^p} = s_p,$$

en multipliant par $x + \frac{1}{x} = y$, on a

(7) $$s_{p+1} = y s_p - s_{p-1},$$

formule qui permet de calculer successivement $s_3, s_4, s_5, \ldots$.

On obtient une formule générale pour le calcul de s_p à l'aide de la théorie des fonctions symétriques. En effet, x et $\frac{1}{x}$ sont racines de l'équation

$$z^2 - yz + 1 = 0.$$

Or on a trouvé [24, (15)]

(8) $$\left\{\begin{aligned} s_p = y^p - p y^{p-2} + \frac{p(p-3)}{1.2} y^{p-4} + \ldots \\ + (-1)^\mu \frac{p(p-\mu+1)\ldots(p-2\mu+1)}{1.2.3\ldots\mu} y^{p-2\mu} + \ldots \end{aligned}\right.$$

Quand le produit de deux racines quelconques d'une équation est égal à k, on abaisse cette équation par la substitution

$$x = u + \frac{k}{u},$$

d'une manière analogue à celle qui permet d'abaisser les équations réciproques.

Exemple :

$$x^7 - 1 = 0;$$

en divisant par $x - 1$, on a

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0,$$

que l'on peut réduire à

$$u^3 + u^2 - 2u - 1 = 0.$$

Exercice. — La substitution

$$x = \frac{a + bu}{1 + u}$$

peut être utilisée pour faire disparaître le deuxième et le troisième terme de l'équation du troisième degré.

Formation des équations dans lesquelles une racine est fonction de plusieurs racines d'une équation donnée.

46. Jusqu'ici, l'équation cherchée avait chacune de ses racines fonction d'une seule racine de la proposée. On peut aussi former des équations dont les racines soient fonctions de plusieurs racines de la proposée. Un exemple de ce cas a été traité lorsque nous avons cherché l'équation aux carrés des différences dans laquelle chaque racine est déterminée par deux racines de la proposée. D'une manière générale, on peut déterminer une racine de l'équation cherchée au moyen de la relation

$$(1) \qquad y = f(x_1, x_2, \ldots, x_p).$$

On obtient alors toutes les racines de l'équation cherchée, en remplaçant les p racines x qui figurent sous le signe f par les racines de la proposée de toutes les manières possibles; si l'on suppose que f soit une fonction rationnelle, cette fonction aura autant de valeurs qu'il y a de manières de prendre p racines parmi celles de la proposée. Si l'on représente les valeurs par $f_1, f_2, \ldots, f_\mu$, l'équation cherchée sera

$$(2) \qquad (y - f_1)(y - f_2)\ldots(y - f_\mu) = 0.$$

Comme le premier membre de cette équation est une fonction symétrique de $f_1, f_2, \ldots, f_\mu$, il sera aussi une fonction symétrique des racines de la proposée et pourra s'exprimer

rationnellement en fonction de ses coefficients. L'équation cherchée aura donc ses coefficients rationnels, si les coefficients de la proposée sont eux-mêmes rationnels, et son degré sera le nombre des valeurs de la fonction f.

47. On peut suivre une autre voie pour trouver l'équation cherchée et faire usage de l'élimination; mais on peut ainsi introduire des solutions étrangères dont il faut se débarrasser. Considérons, par exemple, l'équation générale de degré n et proposons-nous de trouver l'équation dont les racines sont données par la formule

$$y = x_1 + \alpha x_2, \tag{3}$$

où α est un nombre donné; on en tire

$$x_1 = y - \alpha x_2 \tag{4}$$

et, comme x_1 est racine de l'équation donnée $f(x) = 0$,

$$f(y - \alpha x_2) = 0. \tag{5}$$

Si l'on ordonne cette équation et si l'on écrit x au lieu de x_2, on a

$$f(y - \alpha x) = 0, \qquad f(x) = 0. \tag{6}$$

Ces deux équations doivent avoir une racine commune, ce que l'on exprime en éliminant x; la résultante est l'équation cherchée en y.

On voit que les équations (6) auront une racine commune quand on aura

$$y = x_p + \alpha x_q,$$

ce qui n'exclut pas le cas où l'on aurait $x_p = x_q$ contrairement à ce que l'on suppose : l'équation transformée aura donc pour racines étrangères les valeurs de $(1 + \alpha)x_p$; toutes ces quantités sont racines de

$$f\left(\frac{y}{1 + \alpha}\right) = 0$$

et pourront être écartées. Alors la résultante, qui était de

degré n^2, pourra être réduite au degré $n(n-1)$, et aura pour racines les valeurs de $x_1 + \alpha x_2$, x_1 et x_2 étant supposés différents.

Pour $\alpha = 1$, les racines de l'équation finale deviennent égales deux à deux et, par une extraction de racine carrée, cette équation se réduit au degré $\frac{n(n-1)}{2}$, nombre des valeurs distinctes de $x_1 + x_2$.

Plus loin, nous développerons une autre méthode qui permettra de faire usage de l'élimination sans introduire de solutions étrangères. (Voir *Calcul des racines imaginaires des équations numériques.*)

D'une manière analogue, on voit que l'équation qui a pour racines les produits des racines prises deux à deux des racines de l'équation proposée s'obtient en éliminant x entre

$$(9) \qquad f(x) = 0 \quad \text{et} \quad f\left(\frac{y}{x}\right) = 0,$$

la résultante admet comme racines étrangères les carrés des racines de la proposée.

48. On peut utiliser les relations qui existent entre les coefficients et les fonctions symétriques des racines pour écarter de l'expression donnée plusieurs racines et ensuite faire usage de l'élimination. Soit, par exemple, l'équation

$$x^3 + \alpha_1 x^2 + \alpha_2 x + \alpha_3 = 0$$

et

$$y_1 = \frac{x_1}{x_1 + x_2}.$$

Si l'on fait usage de la relation

$$x_1 + x_2 + x_3 = -\alpha_1$$

qui donne

$$y_1 = \frac{-x_1}{\alpha_1 + x_1},$$

on obtient l'équation cherchée en éliminant x entre la proposée et

$$x(y+1) + y\alpha_1 = 0.$$

Si l'on voulait avoir, pour la même équation, l'équation aux carrés des différences, on aurait

$$y = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = (\alpha_1 + x_3)^2 + \frac{4\alpha_3}{x_3},$$

et il faudrait éliminer x entre la proposée et

$$xy = x(\alpha_1 + x)^2 + 4\alpha_3.$$

Méthode de Tschirnaüs pour faire disparaître des termes d'une équation.

49. Soit donnée l'équation

$$(1) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0;$$

posons

$$(2) \qquad y = b_0 + b_1 x + b_2 x^2 + \ldots + b_p x^p,$$

où $p < n$. Si l'on élimine x entre (1) et (2), on obtient une équation de degré n en y, car y a autant de valeurs que x. Pour éliminer x, on peut faire usage des méthodes exposées plus haut; on peut aussi procéder comme il suit : On élève (2) au carré, au cube, etc., en éliminant à l'aide de (1) les puissances de x supérieures à la $(n-1)^{\text{ième}}$, on obtient ainsi une série d'équations de la forme

$$(3) \qquad \begin{cases} y^2 = c_0 + c_1 x + c_2 x^2 + \ldots, \\ y^3 = d_0 + d_1 x + d_2 x^3 + \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \end{cases}$$

remplaçons, dans ces équations, x successivement par toutes les racines de (1); en ajoutant les équations ainsi obtenues et en appelant s_1, s_2, ... les sommes des puissances semblables des racines de (1); S_1, S_2, ... les sommes des puissances semblables des valeurs de y, on aura

$$(4) \qquad \begin{cases} S_1 = nb_0 + b_1 s_1 + b_2 s_2 + \ldots, \\ S_2 = nc_0 + c_1 s_1 + c_2 s_2 + \ldots, \\ S_3 = nd_0 + d_1 s_1 + d_2 s_2 + \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \end{cases}$$

s_1, s_2, ... pourront être calculés en fonction des coefficients de l'équation (1) et, inversement, les coefficients de l'équation cherchée pourront être calculés en fonction de S_1, S_2, ... à l'aide des formules connues. Les coefficients indéterminés b_0, b_1, ..., b_p pourront être déterminés de manière à faire disparaître p coefficients de l'équation en y. Si l'on pose ainsi

$$S_1 = 0, \qquad S_2 = 0, \qquad S_3 = 0,$$

on fera disparaître le deuxième, le troisième et le quatrième terme. La première équation est du premier degré, la deuxième du deuxième degré, la troisième du troisième degré par rapport aux coefficients indéterminés. On voit qu'il faudrait, en apparence, résoudre une équation du sixième degré pour faire disparaître ces trois termes; mais Terrard a montré qu'il suffisait pour cela de résoudre une équation du troisième degré.

La première équation $S_1 = 0$ est homogène et du premier degré en b_0, b_1, ...; à l'aide de cette équation on peut éliminer un coefficient dans $S_2 = 0$ et $S_3 = 0$ qui sont homogènes du deuxième et du troisième degré, et qui ne cessent pas de l'être après l'élimination du coefficient en question. Prenons $p = 4$, on pourra disposer de cinq coefficients; S_2 est alors une fonction homogène du second degré de quatre d'entre eux et peut se mettre sous la forme (*voir* 50)

$$\alpha_1 p_1^2 + \alpha_2 p_2^2 + \alpha_3 p_3^2 + \alpha_4 p_4^2,$$

α_1, α_2, α_3, α_4 étant des nombres connus et p_1, p_2, p_3, p_4 des fonctions linéaires homogènes des coefficients indéterminés. Si l'on pose

$$(5) \qquad \alpha_1 p_1^2 + \alpha_2 p_2^2 = 0, \qquad \alpha_3 p_3^2 + \alpha_4 p_4^2 = 0,$$

on obtient, au moyen d'extractions de racines carrées, deux équations linéaires, à l'aide de ces équations, on pourra faire disparaître deux coefficients indéterminés de $S_3 = 0$; l'un d'eux est arbitraire, l'autre sera déterminé par une équation du troisième degré qui, résolue, fournira les valeurs des autres coefficients.

50. Nous avons admis qu'une fonction homogène du deuxième degré pouvait affecter une certaine forme particulière, et il nous reste à le prouver, ce qui se fait comme il suit :

Soient $x_1, x_2, \ldots, x_n$, n variables; une fonction homogène du deuxième degré de ces variables peut se mettre sous la forme

$$\alpha^2 x_1^2 + 2\alpha P x_1 + Q,$$

où α est un coefficient rationnel ou irrationnel et P et Q sont respectivement du premier et du second degré et ne contiennent pas x_1; cette expression peut se mettre sous la forme

$$(\alpha x_1 + P)^2 + Q - P^2,$$

où $Q - P^2$ est une fonction homogène du deuxième degré qui ne contient pas x_1 et peut être traitée comme la précédente. En continuant ainsi, on décompose la fonction donnée en un nombre de carrés au plus égal au nombre des variables.

Cette démonstration est en défaut lorsque tous les termes de la forme $a x_i^2$ manquent. Dans ce cas, la fonction est de la forme

$$x_1 x_2 + A x_1 + B x_2 = (x_1 + B)(x_2 + A) - AB,$$

où A et B sont indépendants de x_1 et x_2; mais alors on a

$$(x_1 + B + x_2 + A)^2 - (x_1 + B - x_2 - A)^2 = 4(x_1 + B)(x_2 + A),$$

et nous pouvons, en introduisant deux carrés, nous débarrasser de deux variables.

Nous reviendrons plus loin sur cette question.

Si l'on applique la méthode précédente à l'équation du cinquième degré ou à l'équation aux inverses, on obtient les transformées

$$x^5 + ax + b = 0, \qquad x^5 + ax^4 + b = 0.$$

DEUXIÈME PARTIE.

SUR LA SOLUTION ALGÉBRIQUE DES ÉQUATIONS.

CHAPITRE I.

L'ÉQUATION DU TROISIÈME DEGRÉ OU ÉQUATION CUBIQUE.

Méthode de Hudde.

51. L'équation du troisième degré

$$x^3 - 1 = 0 \tag{1}$$

est irréductible. Ses racines sont 1, α et β, et l'on a

$$\alpha = \frac{-1 + i\sqrt{3}}{2}; \qquad \beta = \frac{-1 - i\sqrt{3}}{2}; \tag{2}$$

entre ces racines, on a les relations remarquables

$$1 + \alpha + \beta = 0; \qquad 1 + \alpha^2 + \beta^2 = 0; \qquad \alpha\beta = 1;$$
$$\alpha = \beta^2; \qquad \beta = \alpha^2.$$

L'équation générale du troisième degré, ou équation cubique, est de la forme

$$z^3 + Az^2 + Bz + C = 0;$$

la substitution

$$z = x - \frac{A}{3}$$

la ramène à la forme

$$x^3 + ax + b = 0 \tag{3}$$

que l'on peut résoudre de plusieurs manières.

52. Nous remplacerons x par deux nouvelles inconnues p, q, en posant

$$(4) \qquad x = p + q,$$

l'équation (3) deviendra alors

$$p^3 + q^3 + b + (3pq + a)(p + q) = 0,$$

et sera satisfaite si l'on détermine p et q au moyen des deux équations

$$(5) \qquad p^3 + q^3 = -b; \qquad pq = -\frac{a}{3}.$$

En élevant la dernière au cube, on a

$$(6) \qquad p^3 q^3 = -\left(\frac{a}{3}\right)^3.$$

Il est à remarquer que l'on obtiendrait encore cette dernière équation en remplaçant a par αa ou βa.

p^3 et q^3 sont racines de l'équation

$$(7) \qquad v^2 + bv - \left(\frac{a}{3}\right)^3 = 0,$$

et sont déterminés par les formules

$$(8) \qquad \left\{ \begin{matrix} p^3 \\ q^3 \end{matrix} \right\} = -\frac{b}{2} \pm \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3},$$

d'où l'on conclut

$$(9) \qquad x = \sqrt[3]{-\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}},$$

formule connue sous le nom de formule de *Cardan*. Comme une racine cubique a trois valeurs, on a, pour x, neuf valeurs; il s'est donc introduit six racines étrangères; cela tient à ce que l'on a remplacé la deuxième équation (5) par (6) :

les neuf valeurs sont racines des trois équations

$$(10)\qquad \begin{cases} x^2 + \quad ax + b = 0, \\ x^3 + \alpha a x + b = 0, \\ x^3 + \beta a x + b = 0. \end{cases}$$

Pour séparer les racines de ces équations, nous observerons que chacune d'elles est relative aux hypothèses respectives

$$(11)\qquad pq = -\frac{a}{3}; \qquad pq = -\frac{a\alpha}{3}; \qquad pq = -\frac{a\beta}{3}.$$

Si a et b sont réels, p et q doivent être choisis de telle sorte que leur produit soit réel. Nous avons trois cas à considérer :

1° $\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 > 0$, p^3 et q^3 sont réels, p et q ont un système de valeurs réelles; si l'on désigne ces valeurs réelles par p_1 et q_1, tous les systèmes des valeurs de p et q seront

$$(12)\qquad p_1,\quad p_1\alpha,\quad p_1\beta;\quad q_1,\quad q_1\alpha,\quad q_1\beta,$$

et l'équation proposée aura pour racines

$$x_1 = p_1 + q_1; \qquad x_2 = p_1\alpha + q_1\beta; \qquad x_3 = p_1\beta + q_1\alpha,$$

de manière que pq soit réel dans tous les cas. La deuxième et la troisième équation (10) auront pour racines

$$\begin{aligned} &p_1 + q_1\alpha; \quad p_1\alpha + q_1; \quad p_1\beta + q_1\beta, \\ &p_1 + q_1\beta; \quad p_1\beta + q_1; \quad p_1\alpha + q_1\alpha. \end{aligned}$$

On peut aussi poser

$$(13)\qquad x = p - \frac{a}{3p} \qquad \text{ou} \qquad x = q - \frac{a}{3q},$$

et l'on n'obtient alors que les véritables racines. Dans le cas que nous venons d'examiner, l'équation a une racine réelle et deux racines imaginaires.

2° Si $\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 = 0$, p_1 et q_1 sont égaux, l'équation a ses racines réelles; mais deux d'entre elles sont égales.

3° $\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 < 0$. Dans ce cas, p^3 et q^3 sont imaginaires, p et q sont également imaginaires, mais on peut accoupler leurs valeurs de manière que $pq = -\frac{a}{3}$ soit réel; soient p_1 et q_1 de telles valeurs. Les formules (12) fourniront encore les racines, même lorsque a et b sont imaginaires.

Quand a et b sont réels, les racines affecteront une forme imaginaire; il est facile de montrer qu'elles sont réelles. On a, en effet,

$$(14)\qquad \begin{cases} p^3 = -\frac{b}{2} + i\sqrt{-\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3}, \\ q^3 = -\frac{b}{2} - i\sqrt{-\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3}. \end{cases}$$

Si l'on pose alors

$$(15)\qquad -\frac{b}{2} = r\cos\theta, \qquad +\sqrt{-\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3} = r\sin\theta,$$

on trouve

$$(16)\qquad p^3 = r(\cos\theta + i\sin\theta); \qquad q^3 = r(\cos\theta - i\sin\theta),$$

où

$$(17)\qquad r = \sqrt{-\left(\frac{a}{3}\right)^3}; \qquad \cos\theta = \frac{-\frac{b}{2}}{\sqrt{-\left(\frac{a}{3}\right)^3}}$$

θ est donc dans le premier ou le second quadrant, car $\sin\theta$ est positif. On a alors

$$(18)\qquad \begin{cases} p = \sqrt{-\frac{a}{3}}\left(\cos\frac{2k\pi+\theta}{3} + i\sin\frac{2k\pi+\theta}{3}\right), \\ q = \sqrt{-\frac{a}{3}}\left(\cos\frac{2k\pi+\theta}{3} - i\sin\frac{2k\pi+\theta}{3}\right), \end{cases}$$

et

$$x = 2\sqrt{-\frac{a}{3}}\cos\frac{2k\pi+\theta}{3},$$

où k doit recevoir les valeurs 0, 1, 2.

Les trois racines, dans le cas qui vient de nous occuper, sont donc réelles et inégales. On lui donne le nom de cas *irréductible*. On ne peut représenter les racines au moyen de radicaux que sous une forme imaginaire.

Lorsque l'on essaye de calculer p et q sous la forme

$$A \pm B\sqrt{-1}$$

sans faire usage de fonctions trigonométriques, on est fatalement ramené à l'équation donnée.

Méthode de Lagrange.

53. Lagrange cherche à déterminer une fonction des racines qui, une fois connue, permette d'en utiliser les racines. La fonction considérée par Lagrange est

$$(1) \qquad y = (x_1 + \alpha x_2 + \beta x_3)^3,$$

où x_1, x_2, x_3 sont les racines de l'équation proposée et α, β les racines cubiques imaginaires de l'unité. Cette fonction dépend d'une équation du second degré; en effet, elle n'a que deux valeurs, car les six valeurs qu'elle semble prendre quand on y permute les racines ne sont pas distinctes; ainsi, on a (51)

$$x_1 + \alpha x_2 + \beta x_3 = \alpha(\beta x_1 + x_2 + \alpha x_3) = \beta(\alpha x_1 + \beta x_2 + x_3),$$

et

$$(x_1 + \alpha x_2 + \beta x_3)^3 = (\beta x_1 + x_2 + \alpha x_3)^3 = (\alpha x_1 + \beta x_2 + x_3)^3$$

y n'a donc, en réalité, que deux valeurs distinctes, soit

$$y_1 = (x_1 + \alpha x_2 + \beta x_3)^3, \qquad y_2 = (\alpha x_1 + x_2 + \beta x_3)^3,$$

dont la somme et le produit peuvent s'exprimer rationnellement au moyen des coefficients de l'équation. On trouve

$$y^2 + 27by - 27a^3 = 0,$$

et les racines sont données par les formules

$$x_1 + x_2 + x_3 = 0;$$
$$x_1 + \alpha x_2 + \beta x_3 = \sqrt[3]{y_1};$$
$$\alpha x_1 + x_2 + \beta x_3 = \sqrt[3]{y_2};$$

Nous ne ferons pas de discussion.

Méthodes de Tschirnaüs et d'Euler.

54. Ces deux méthodes, au fond, rentrent l'une dans l'autre; en posant

(1) $$y^2 + py + q = x,$$

et en choisissant p et q de manière qu'en éliminant y entre cette équation et

(2) $$y^3 = d,$$

on trouve l'équation proposée. On peut aussi se proposer de ramener l'équation à la forme (2) en posant

$$x = \frac{p + qy}{1 + y}.$$

Exemple :

$$x^3 + x^2 - 2x - 1 = 0,$$

$$x = y - \frac{1}{3}; \qquad y^3 - \frac{7}{3}y - \frac{7}{27} = 0, \qquad \left(\frac{7}{54}\right)^2 - \left(\frac{7}{9}\right)^3 < 0.$$

$$\cos\theta = \frac{\frac{7}{54}}{\sqrt{\left(\frac{7}{9}\right)^3}} = \frac{1}{2\sqrt{7}}; \qquad \theta = 79^\circ 6' 24''.$$

$$y = \frac{2}{3}\sqrt{7}\cos\frac{2p\pi + \theta}{3}.$$

Problème. — Quelles sont les équations irréductibles du troisième degré dont une racine peut s'exprimer rationnellement au moyen d'une autre?

Si x_1 et x_2 désignent les deux racines, on pourra poser

$$x_1 = a + bx_2 + cx_2^2,$$

car toute fonction rationnelle d'une racine affectera cette forme (26).

Soit

$$f(x) = x^3 + px^2 + qx + r = 0$$

l'équation demandée et $\Psi(x) = 0$ l'équation qui a pour racines les trois valeurs de $a + bx_2 + cx_2^2$; $f(x) = 0$ et $\Psi(x) = 0$ ont alors une racine commune et, comme $f(x)$ est irréductible, toutes leurs racines doivent être égales deux à deux; comme on ne peut pas avoir, par exemple,

$$x_3 = a + bx_3 + cx_3^2,$$

car x_3 serait racine d'une équation du second degré, il faut que l'on ait

$$x_1 = a + bx_2 + cx_2^2,$$
$$x_2 = a + bx_3 + cx_3^2,$$
$$x_3 = a + bx_1 + cx_1^2.$$

On tire de ces équations

$$c = \frac{p^2 - 3q}{\sqrt{\mathrm{D}}}$$

où

$$\mathrm{D} = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_2 - x_1)^2 \quad (\textit{voir } 25).$$

b et a contiennent $\sqrt{\mathrm{D}}$ au dénominateur; mais ils ne contiennent pas d'autre irrationnalité. Toutes les équations du troisième degré pour lesquelles $\sqrt{\mathrm{D}}$ sera censé connu jouiront alors de la propriété demandée; en prenant $\sqrt{\mathrm{D}}$ successivement avec le signe $+$ et avec le signe $-$, on aura deux racines en fonction de la troisième.

CHAPITRE II.

L'ÉQUATION DU QUATRIÈME DEGRÉ OU ÉQUATION BIQUADRATIQUE.

Méthode de Lagrange.

55. La résolution de l'équation du quatrième degré s'effectue au moyen d'une équation du troisième degré, que l'on appelle la *résolvante*. L'inconnue de cette dernière équation est une fonction des racines de la proposée qui n'a que trois valeurs. Il existe plusieurs fonctions jouissant de cette propriété, par exemple

$$x_1 x_2 + x_3 x_4,$$
$$(x_1 + x_2)(x_3 + x_4),$$
$$(x_1 - x_2 + x_3 - x_4)^2.$$

Lagrange fait usage de la première; il pose

$$(1) \quad y_1 = x_1 x_2 + x_3 x_4; \qquad y_2 = x_1 x_3 + x_2 x_4; \qquad y_3 = x_1 x_4 + x_2 x_3.$$

Si l'équation donnée est

$$(2) \qquad f(x) = x^4 + Ax^3 + Bx^2 + Cx + D = 0,$$

on a

$$y_1 + y_2 + y_3 = B,$$
$$y_1 y_2 + y_1 y_3 + y_2 y_3 = \Sigma x_1^2 x_2 x_3 = AC - 4D,$$
$$y_1 y_2 y_3 = \Sigma x_1^3 x_2 x_3 x_4 + \Sigma x_1^2 x_2^2 x_3^2 = D(A^2 - 4B) + C^2;$$

la résolvante est alors

$$(3) \qquad y^3 - By^2 + (AC - 4D)y + D(4B - A^2) - C^2 = 0.$$

Méthode de Descartes.

56. Descartes pose

$$f(x) = (x^2 + \alpha_1 x + \alpha_2)(x^2 + \beta_1 x + \beta_2)$$

et l'identification lui donne

$$\begin{aligned} \alpha_1 + \beta_1 &= A, \\ \alpha_1\beta_1 + \alpha_2 + \beta_2 &= B, \\ \alpha_1\beta_2 + \beta_1\alpha_2 &= C, \\ \alpha_2\beta_2 &= D. \end{aligned}$$

Si l'on fait alors

$$\alpha_2 + \beta_2 = y,$$

et si l'on élimine α_1, β_1, α_2, β_2 entre ces cinq équations, on trouve une équation en y identique à celle que nous avons obtenue plus haut. Cela s'explique en observant que α_2 et β_2 sont les produits de couples de racines et $\alpha_2 + \beta_2$ est la fonction utilisée par Lagrange; on pourrait tout aussi bien poser

$$y = \alpha_1\beta_1 \qquad \text{ou} \qquad y = (\alpha_1 - \beta_1)^2,$$

et y serait toujours une des fonctions possédant trois valeurs identiques à celles que nous avons citées plus haut.

Méthode de Ferrari.

57. Ferrari, qui a le premier résolu l'équation du quatrième degré est parvenu à la même résolvante que Lagrange et que Descartes. Il écrit l'équation sous la forme

$$(1) \quad \left(x^2 + \frac{A}{2}x + \frac{y}{2}\right)^2 = \left(\frac{A^2}{4} - B + y\right)x^2 + \left(\frac{Ay}{2} - C\right)x + \frac{y^2}{4} - D,$$

et il détermine y de manière à rendre le second membre égal à un carré parfait; en écrivant cette condition, on retrouve la résolvante de Lagrange, et y a encore la même signification que plus haut. Si l'on désigne par S^2 le second membre

de (1), lorsque y a été déterminé comme on vient de le dire, on a

$$(2) \qquad x^2 + \frac{A}{2}x + \frac{y}{2} \pm S = 0,$$

et l'équation du quatrième degré se décompose en deux autres du second degré qui fournissent les racines cherchées; on a ainsi

$$x_1 x_2 = \frac{y}{2} + S, \qquad x_3 x_4 = \frac{y}{2} - S;$$

et, par suite,

$$y = x_1 x_2 + x_3 x_4.$$

Méthodes de Tschirnaüs et d'Euler.

58. Tschirnaüs ramène l'équation à la forme

$$y^4 + Py^2 + Q = 0$$

en posant

$$y = a + bx + x^2$$

et il détermine a et b de manière à annuler les coefficients de y^3 et de y.

Euler élimine y entre

$$x = a + by + cy^2 + dy^3$$

et

$$y^4 = e,$$

et détermine a, b, c, d et e de manière que la résultante coïncide avec l'équation proposée. Nous n'indiquerons pas comment les racines de la proposée dépendent de l'équation du troisième degré que l'on obtient ainsi. Euler a aussi indiqué une méthode analogue à celle de Hudde pour le troisième degré en posant

$$x = p + q + r;$$

on peut disposer de p, q, r de manière à décomposer l'équation en trois autres qui font connaître $p^2+q^2+r^2$, $p^2q^2+p^2r^2+q^2r^2$,

et pqr; p^2, q^2 et r^2 sont alors racines d'une même équation du troisième degré.

Étude approfondie de la méthode de Descartes.

59. Dans la pratique, il convient de donner la préférence à la méthode de Descartes, en la modifiant un peu. On ramènera d'abord l'équation à la forme

$$x^4 + ax^2 + bx + c = 0, \tag{1}$$

et l'on posera

$$x^4 + ax^2 + bx + c = (x^2 + \alpha x + \beta)(x^2 - \alpha x + \gamma), \tag{2}$$

et, par suite,

$$-\alpha^2 + \beta + \gamma = a, \qquad \alpha(\gamma - \beta) = b, \qquad \beta\gamma = c, \tag{3}$$

on en déduit

$$\beta + \gamma = a + \alpha^2,$$

$$\gamma - \beta = \frac{b}{\alpha},$$

$$4\beta\gamma = 4c = (a + \alpha^2)^2 - \frac{b^2}{\alpha^2},$$

ou

$$\alpha^6 + 2a\alpha^4 + (a^2 - 4c)\alpha^2 - b^2 = 0; \tag{4}$$

cette équation, en posant $\alpha^2 = y$, devient

$$y^3 + 2ay^2 + (a^2 - 4c)y - b^2 = 0; \tag{5}$$

l'équation en α a six racines, à savoir les six valeurs de $x_1 + x_2$; elles sont, par couples, égales et de signes contraires, car (1) donne

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Si a et b sont réels, le dernier terme de la résolvante est négatif; elle a donc toujours une racine positive et les deux autres sont toutes deux positives, négatives ou imaginaires; $\alpha = \sqrt{y}$ sera alors réel au moins pour une valeur de y; or

$$\beta = \frac{a + \alpha^2}{2} - \frac{b}{2\alpha} : \tag{6}$$

deux racines seront donc fournies par l'équation

$$x^2 + \alpha x + \frac{\alpha^3 + a\alpha - b}{2\alpha} = 0, \tag{7}$$

et l'on obtient les deux autres en changeant α en $-\alpha$.

On voit que les racines de l'équation proposée sont données par de simples extractions de racines carrées, si la résolvante a une racine rationnelle, et cette condition, comme on le verra plus tard, est nécessaire et suffisante pour que l'on puisse résoudre la proposée au moyen de racines carrées.

Si l'on a

$$\frac{\alpha^2}{4} + \frac{a}{2} > \frac{b}{2\alpha}$$

pour les deux valeurs, l'équation (7) du second degré montre que les quatre racines sont imaginaires; elles sont toutes réelles si l'on a, au contraire,

$$\frac{\alpha^2}{4} + \frac{a}{2} < \pm \frac{b}{2\alpha},$$

et, si $\frac{\alpha^2}{4} + \frac{a}{2}$ est compris entre $+$ et $-\frac{b}{2\alpha}$, deux racines sont réelles et deux autres imaginaires.

Si l'équation proposée a des racines égales, les deux équations du second degré considérées plus haut auront une racine commune, ou bien l'une d'elles aura une racine double; dans ce dernier cas, on a

$$\frac{\alpha^2}{4} + \frac{a}{2} = \pm \frac{b}{2\alpha}$$

ou

$$\left(\frac{\alpha^2}{4} + \frac{a}{2}\right)^2 = \frac{b^2}{4\alpha^2},$$

et, comme on a $\alpha^2 = y$, on peut écrire cette équation

$$y\left(\frac{y}{2} + a\right)^2 - b^2 = 0.$$

Cette équation devant avoir une racine commune avec la ré-

solvante, celle-ci doit être réductible. On arrive à la même conclusion en admettant que les équations du deuxième degré ont une racine commune.

60. Nous avons vu que nous n'avions besoin de connaître qu'une seule racine de la résolvante pour en déduire toutes les racines de la proposée; on peut aussi utiliser toutes les racines de la résolvante; appelons-les α_1^2, α_2^2, α_3^2, on aura

$$\alpha_1^2+\alpha_2^2+\alpha_3^2=-2a, \qquad \alpha_1^2\alpha_2^2\alpha_3^2=b^2 \qquad \text{ou} \qquad \alpha_1\alpha_2\alpha_3=b,$$

car on peut choisir α_1, α_2, α_3 de telle sorte que leur produit ait le signe de b.

La quantité placée sous le radical dans les racines de

$$x^2+\alpha x+\beta=0$$

peut prendre une autre forme; on a, pour $\alpha=\alpha_1$,

$$-\frac{\alpha^2}{4}-\frac{a}{2}+\frac{b}{2\alpha}=\frac{(\alpha_2+\alpha_3)^2}{4},$$

et alors

$$\left.\begin{matrix}x_1\\x_2\end{matrix}\right\}=\frac{-\alpha_1\pm(\alpha_2+\alpha_3)}{2}; \tag{8}$$

de même

$$\left.\begin{matrix}x_3\\x_4\end{matrix}\right\}=\frac{\alpha_1\pm(\alpha_2+\alpha_3)}{2}. \tag{9}$$

La résolvante a toujours une racine positive; soit α_1^2 cette racine, et α_1 la valeur positive de $\sqrt{\alpha_1^2}$. $\alpha_2\alpha_3$ doit alors avoir le signe de b; trois cas peuvent se présenter :

1° α_2^2 et α_3^2 *sont tous deux positifs*. α_2 et α_3 ont le même signe si b est positif; ils sont de signes contraires si b est négatif : les racines de la proposée sont toutes réelles.

2° α_2^2 et α_3^2 *sont tous deux négatifs*. On posera

$$\alpha_2^2=-m, \qquad \alpha_3^2=-n,$$

m et n étant positifs; on a alors

$$\alpha_2=\mp i\sqrt{m}; \qquad \alpha_3=\pm i\sqrt{n}$$

si b est positif et

$$\alpha_2 = \pm i\sqrt{m}, \qquad \alpha_3 = \pm i\sqrt{n}$$

si b est négatif; *les racines de la proposée sont imaginaires* dans le cas où m et n sont inégaux. Si $m = n$, *deux racines sont égales, les deux autres imaginaires.*

3° α_2^2 et α_3^2 *sont tous deux imaginaires;* alors on posera

$$\alpha_2^2 = r^2(\cos\theta + i\sin\theta); \qquad \alpha_3^2 = r^2(\cos\theta - i\sin\theta)$$

et

$$\alpha_2 = \pm r\left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\right);$$

$$\alpha_3 = \pm r\left(\cos\frac{\theta}{2} - i\sin\frac{\theta}{2}\right),$$

et les signes de r seront les mêmes ou non, suivant que b sera positif ou négatif; dans le premier cas, on a

$$\left.\begin{matrix} x_1 \\ x_2 \end{matrix}\right\} = \frac{-\alpha_1 \pm 2r\cos\frac{\theta}{2}}{2},$$

$$\left.\begin{matrix} x_3 \\ x_4 \end{matrix}\right\} = \frac{\alpha_1 \pm 2ir\sin\frac{\theta}{2}}{2};$$

dans le second,

$$\left.\begin{matrix} x_1 \\ x_2 \end{matrix}\right\} = \frac{-\alpha_1 \pm 2ir\sin\frac{\theta}{2}}{2},$$

$$\left.\begin{matrix} x_3 \\ x_4 \end{matrix}\right\} = \frac{\alpha_1 \pm 2r\cos\frac{\theta}{2}}{2}:$$

l'équation proposée a alors deux racines réelles et deux racines imaginaires.

CHAPITRE III.

L'ÉQUATION BINOME.

Expression des racines au moyen des lignes trigonométriques.

61. On appelle équations binomes les équations de la forme

$$z^n = a. \tag{1}$$

Nous avons déjà rencontré des cas particuliers de cette équation; nous allons maintenant nous occuper du cas général.

Si a est imaginaire, par exemple, si

$$a = a_1 + i b_1, \tag{2}$$

on pose

$$a_1 = r\cos\theta, \qquad b_1 = r\sin\theta; \tag{3}$$

on trouve

$$z = \sqrt[n]{r}\left(\cos\frac{2p\pi + \theta}{n} + i\sin\frac{2p\pi + \theta}{n}\right). \tag{4}$$

Cette formule donne les n valeurs de z en attribuant à p n valeurs entières consécutives. Les racines sont imaginaires, car, pour obtenir une valeur réelle, il faudrait avoir, pour une valeur entière de p,

$$\frac{2p\pi + \theta}{n} = k\pi,$$

k désignant un entier, ce qui ne peut avoir lieu que si $\theta = 0$ ou $\theta = \pi$, ce qui suppose $b = 0$.

Si a est réel et si k désigne le nombre positif tel que

$$k^n = \pm a,$$

l'équation (1), en posant

$$z = kx,$$

devient

$$x^n = \pm 1.$$

On obtient, comme plus haut, pour les racines de

$$x^n = 1, \tag{5}$$

$$x = \cos\frac{2p\pi}{n} + i\sin\frac{2p\pi}{n}, \tag{6}$$

et pour celles de

$$x^n = -1, \tag{7}$$

$$x = \cos\frac{(2p+1)\pi}{n} + i\sin\frac{(2p+1)\pi}{n}. \tag{8}$$

Dans le premier cas, on obtient une racine réelle pour $2p\pi = 0$ ou $2p\pi = n\pi$, en attribuant à p les valeurs

$$0, \quad 1, \quad 2, \quad \ldots, \quad (n-1).$$

Si n est impair, on ne peut prendre que $p = 0$, ce qui donne $x = 1$; si n est pair, on peut prendre $p = 0$ et $p = \frac{n}{2}$, d'où l'on tire $x = 1$ et $x = -1$. Les autres racines sont imaginaires et conjuguées deux à deux.

Dans le second cas, on a des racines réelles en prenant

$$2p + 1 = 0, \qquad \text{et} \qquad 2p + 1 = n;$$

la première équation n'a pas de solution, et la seconde n'en a que si n est impair; si n est pair, on n'a que des racines imaginaires; si n est impair, on n'a qu'une racine réelle $x = -1$; les racines imaginaires sont encore ici conjuguées deux à deux.

Propriétés des racines.

62. Les racines des équations binomes jouissent de propriétés dont on fait un fréquent usage; nous considérerons spécialement l'équation

$$x^n = 1.$$

Les racines communes aux équations

$$x^n = 1 \qquad \text{et} \qquad x^m = 1$$

sont racines de l'équation

$$x^q = 1,$$

où q est le plus grand commun diviseur de m et *n.*

Cela résulte de ce que $x^q - 1$ est le plus grand commun diviseur de $x^m - 1$ et $x^n - 1$.

63. *Toute puissance d'une racine de l'équation*

$$x^n = 1$$

est une racine de cette équation.

Car si α est une racine de $x^n = 1$, α^p sera aussi une racine, puisque $(\alpha^p)^n = (\alpha^n)^p = 1$.

64. *Si p est un nombre premier, toutes les racines de*

$$x^p = 1$$

pourront être représentées par

$$\alpha, \quad \alpha^2, \quad \alpha^3, \quad \ldots, \quad \alpha^p,$$

α désignant une quelconque des racines.

Comme tous les termes de cette suite sont racines, il suffit de montrer qu'ils sont tous inégaux. Or, si l'on pouvait avoir

$$\alpha^q = \alpha^r,$$

où $q > r$, on aurait ainsi

$$\alpha^r(\alpha^{q-r} - 1) = 0,$$

et comme α n'est pas nul, α devrait être racine de

$$x^{q-r} - 1 = 0;$$

ce qui est impossible, car (62) $q - r < p$ et l'équation précédente ne peut avoir d'autre racine commune avec la proposée que l'unité. Si p n'est pas un nombre premier, plusieurs termes de la suite $\alpha, \alpha^2, \alpha^3, \ldots$ pourront être égaux, en sorte que cette suite ne fournira pas nécessairement toutes les racines.

On appelle racines primitives celles qui ne satisfont à aucune autre équation de la forme $x^q = 1$, où q est moindre que p. Si p est un nombre premier, toutes les racines sont primitives, excepté l'unité. Si p n'est pas premier et si α est une racine primitive, toutes les racines sont comprises dans la suite $\alpha, \alpha^2, \alpha^3, \ldots,$ qui sont déterminées par des équations binomes. Si p est une puissance de nombre premier, toutes les racines sont primitives, à l'exception de celles dont l'exposant est une puissance de p inférieure au degré de l'équation. Ainsi $-i$ et $+i$ sont racines primitives pour $p = 4$, alors que -1 et $+1$ ne le sont pas, vu qu'ils sont racines de $x^2 = 1$. Toutes les racines peuvent être représentées par α, α^2, α^3, α^4, si $\alpha = \pm i$; mais non si $\alpha = \pm 1$.

On peut démontrer comme il suit qu'il existe pour toute valeur de n des racines primitives; si, en effet, toutes les racines pouvaient satisfaire à des équations de degré moindre que le degré de la proposée, on aurait pour chaque valeur de p

$$\frac{2p\pi}{n} = \frac{2p_1\pi}{n_1},$$

où $n_1 < n$; ce qui ne peut avoir lieu que si $\frac{p}{n}$ est réductible à une plus simple expression. *Il y a donc autant de racines primitives que de nombres entiers inférieurs à n et premiers avec n*; ce nombre est, comme l'on sait, égal à

$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_q}\right),$$

$p_1, p_2, \ldots, p_q$ étant les facteurs premiers de n.

65. *Si m et n sont premiers entre eux, on obtient toutes les racines de $x^{mn}=1$ en multipliant toutes les racines de $x^m=1$ par toutes les racines de $x^n=1$.*

En effet, si les arguments des racines de $x^m=1$ et $x^n=1$ sont $\frac{2p\pi}{m}$ et $\frac{2q\pi}{n}$ l'argument de leur produit sera $\frac{2\pi(qm+pn)}{mn}$. Ce produit sera donc racine de $x^{mn}=1$; il reste à prouver que tous les mn résultats ainsi obtenus sont différents. S'ils ne l'étaient pas, on aurait, par exemple,

$$qm+pn=q_1m+p_1n$$

ou

$$\frac{m}{n}=\frac{p_1-p}{q-q_1},$$

ce qui est impossible, car m et n sont premiers entre eux et $p_1-p<m$, $q-q_1<n$.

On voit facilement que ce théorème peut être étendu à un nombre quelconque d'équations binomes dans lesquelles les exposants de l'inconnue sont premiers entre eux. Les équations de la forme $x^n=1$ peuvent donc être ramenées à d'autres dans lesquelles les exposants de l'inconnue sont des puissances de nombres premiers.

66. *L'équation*

$$x^{p^\mu}=1,$$

où p désigne un nombre premier, peut être résolue à l'aide d'équations de la forme

$$x^p=\alpha.$$

En effet, l'équation proposée peut être résolue au moyen des suivantes

$$x^p=\alpha_1;\qquad \alpha_1^p=\alpha_2,\qquad \alpha_2^p=\alpha_3,\qquad \ldots,\qquad \alpha_{\mu-1}^p=1.$$

Si, en résolvant ces équations, on prend une racine quelconque, pourvu qu'elle ne soit pas égale à 1, la valeur de x, à laquelle on parvient de cette manière, est une racine primitive de la proposée, sans quoi elle donnerait, pour l'une des

quantités α_1, α_2, ..., la valeur 1, ce qui est contraire à nos hypothèses; on trouve, de cette manière, une racine primitive de la proposée, et ses puissances donnent les autres racines.

Nous venons ainsi de prouver que toute équation de la forme

$$x^n = 1$$

peut être ramenée à des équations la forme

$$x^p = \alpha,$$

où p est un facteur premier de n, α étant déterminé comme on vient de le dire.

67. Les fonctions symétriques des racines de $x^n - 1 = 0$ sont faciles à calculer; on a, en effet,

$$s_p = x_1^p + x_2^p + \ldots + x_n^p = \alpha^p + \alpha^{2p} + \ldots + 1,$$

ou

$$s_p = \frac{1 - \alpha^{np}}{1 - \alpha^p},$$

α désignant une racine primitive. Si p n'est pas divisible par n, le numérateur de la fraction est nul, le dénominateur ne l'est pas, ainsi $s_p = 0$. Si p est divisible par n, la fraction prend une forme indéterminée; mais chaque terme de s_p est égal à l'unité, donc $s_p = n$. Il en résulte

$$\Sigma x_1^\alpha x_2^\beta x_3^\gamma \ldots = 0,$$

toutes les fois que $\alpha + \beta + \gamma + \ldots$ n'est pas divisible par n; car une pareille fonction s'exprime sous forme de sommes de termes tels que $s_p s_q s_r \ldots$, qui sont nuls dès que les indices ne sont pas tous divisibles par n, et la somme des indices est égale à la somme des exposants de la fonction.

Application de la théorie des équations réciproques aux équations binomes.

68. L'application de la théorie des équations réciproques à l'équation binome permet d'abaisser le degré de cette équa-

tion. Considérons l'équation

$$x^p = 1, \tag{1}$$

où p désigne un nombre premier; tous les cas où p n'est pas premier pouvant se ramener à celui-ci.

Soit $p = 2n + 1$; en divisant par $x - 1$, on a

$$x^{2n} + x^{2n-1} + x^{2n-2} + \ldots + x + 1 = 0; \tag{2}$$

cette équation est réciproque et la substitution

$$y = x + \frac{1}{x}$$

conduit à une équation de degré n

$$U_n = 0. \tag{3}$$

Cette équation a toutes ses racines réelles; en effet, on a

$$x^2 - xy + 1 = 0; \tag{4}$$

il en résulte que, à une valeur de y correspondent deux valeurs de x dont la somme est y et le produit 1. Deux racines jouissant de cette propriété sont données par les formules

$$x_1 = \cos\frac{2p_1\pi}{2n+1} + i\sin\frac{2p_1\pi}{2n+1},$$

$$x_2 = \cos\frac{2p_1\pi}{2n+1} - i\sin\frac{2p_1\pi}{2n+1},$$

en sorte que

$$y = 2\cos\frac{2p_1\pi}{2n+1}. \tag{5}$$

Les racines de l'équation (3) sont donc les n valeurs différentes de $2\cos\frac{2p_1\pi}{2n+1}$ que l'on obtient en posant

$$p_1 = 1, 2, \ldots, n.$$

Dans cette expression, les arcs sont des multiples de la $(2n+1)^{\text{ième}}$ partie de la circonférence; ces arcs peuvent être construits à l'aide de lignes droites et d'arcs de cercle, si

leurs cosinus peuvent s'obtenir par des extractions de racines carrées. On voit ainsi que le problème, qui a pour but de partager la circonférence en p parties égales au moyen d'arcs de cercle et de lignes droites, revient à résoudre l'équation

$$x^p - 1 = 0,$$

au moyen d'extractions de racines carrées. Pour $p = 5$, l'équation en y est du deuxième degré et le problème admet une solution. Pour $p = 7$, l'équation en y est du troisième degré et ne peut être résolue au moyen de racines carrées.

Plus loin, nous reprendrons cette question; pour le moment, nous nous bornerons à établir le théorème suivant :

69. *Si p est un nombre premier, l'équation*

$$\frac{x^p - 1}{x - 1} = 0$$

est irréductible.

Si X est un polynome entier à coefficients entiers, décomposable en facteurs A, B de degrés moindres, A et B pourront avoir leurs coefficients entiers. En effet, si l'on avait l'identité

$$X = AB,$$

A et B ayant des coefficients fractionnaires, on pourrait multiplier par un nombre k et faire perdre aux coefficients leur forme fractionnaire; maintenant kX est divisible par un facteur premier de k, il doit en être de même de A ou B ([1]); on pourra diviser les deux membres de l'équation par ce facteur sans introduire de dénominateurs et ainsi de suite.

Maintenant, supposons que

$$\frac{x^p - 1}{x - 1}$$

([1]) La démonstration qu'on donne ordinairement de ce théorème, A et B étant des nombres entiers, s'applique encore au cas où A et B sont des polynomes à coefficients entiers. Le polynome est dit *divisible* par x, si tous ses coefficients sont divisibles par x.

soit le produit de deux facteurs rationnels; ces facteurs devront avoir leurs coefficients entiers; changeons x en $x+1$, l'expression précédente prendra la forme

$$(6)\qquad x^{p-1}+p\varphi(x)+p,$$

$\varphi(x)$ désignant un polynome entier rationnel à coefficients entiers et divisibles par x; les termes indépendants de x dans les facteurs de (6) ayant pour produit p, et p étant un nombre premier, devront être égaux à ± 1 et à $\pm p$; le produit en question aura donc la forme

$$(\pm 1+a_1x+a_2x^2+\ldots)(\pm p+b_1x+b_2x^2+\ldots);$$

retranchons des deux membres de l'équation

$$\pm p(\pm 1+a_1x+a_2x^2\ldots);$$

tous les termes de ce qui reste dans (6), à l'exception de x^{p-1}, seront divisibles par p; il en résulte que b_1 est divisible par p, et ainsi de suite; en continuant ainsi, on arrive à une égalité de la forme

$$(\pm 1+a_1x+a_2x^2\ldots)x^\mu=x^{p-1}+p\varphi_1(x),$$

d'où il résulterait que p devrait diviser le coefficient de x^μ, ce qui est impossible, puisqu'il est égal à ± 1; l'équation en question est donc irréductible.

CHAPITRE IV.

L'ÉQUATION DU CINQUIÈME DEGRÉ.

Impossibilité de résoudre cette équation algébriquement.

70. On a vu que la résolution de l'équation du troisième et du quatrième degré réussit, grâce à cette circonstance qu'il est possible de trouver une fonction des racines possédant moins de valeurs qu'une racine même, et qui, par conséquent, dépend d'une équation de degré moindre. Lagrange a montré que lorsque l'on essayait d'appliquer les méthodes qui réussissent pour le troisième et le quatrième degré à des équations de degré supérieur, l'équation auxiliaire était de degré supérieur à celui de la proposée. Il devenait ainsi probable que les équations générales de degré supérieur au quatrième ne pouvaient pas avoir de racines algébriquement exprimables en fonction des coefficients. Abel a montré qu'il en était réellement ainsi. Sa démonstration a été simplifiée par Galois. Nous allons exposer la démonstration de Galois en la modifiant dans la forme.

Si une équation générale du degré n pouvait être résolue à l'aide de radicaux, il en serait de même de l'équation

$$(1)\quad \begin{cases} x^n - (x_1 + x_2 \ldots + x_n)\, x^{n-1} \\ \quad + x_1 x_2 + x_1 x_3 \ldots)\, x^{n-2} \ldots \pm x_1 x_2 \ldots x_n = 0, \end{cases}$$

où x_1, x_2, ..., x_n sont arbitraires et indépendantes les unes des autres. x_1, x_2, ..., x_n étant les racines de l'équation, la résolution doit conduire à ces valeurs. Toute racine que l'on aura besoin d'extraire devra pouvoir s'effectuer quand

on remplacera les coefficients a_1, a_2, ... par leurs valeurs en x_1, x_2, ..., x_n.

Maintenant, supposons que la première racine à extraire soit

$$y = \sqrt[r]{A};$$

A ne contient pas de radicaux, c'est une fonction des coefficients de l'équation, et, par suite, une fonction symétrique de x_1, x_2, ..., x_n. Mais y ne peut pas être une fonction symétrique rationnelle de x_1, x_2, ..., x_n, sans quoi il s'exprimerait rationnellement au moyen des coefficients; si y n'est pas symétrique, il contiendra deux racines x_1 et x_2, qui, en se permutant, changeront la valeur de y; comme toutes les valeurs de y sont données par la formule

$$y^r = A,$$

l'une des valeurs doit se déduire d'une autre en la multipliant par une valeur α de $1^{\frac{1}{r}}$ différente de l'unité. Si donc $f(x_1, x_2, \ldots)$ est l'une des valeurs de y, on aura

$$f(x_1, x_2, x_3, x_4, \ldots, x_n) = \alpha f(x_2, x_1, x_3, x_4, \ldots, x_n).$$

Cette équation doit être identique, car x_1, x_2, ... sont indépendantes les unes des autres; elle subsiste donc en permutant x_1 et x_2; on obtient alors

$$f(x_2, x_1, x_3, x_4, \ldots, x_n) = \alpha f(x_1, x_2, x_3, x_4, \ldots, x_n);$$

en multipliant cette équation par la précédente, on a

$$\alpha^2 = 1, \qquad \alpha = -1.$$

On peut toujours supposer que p est premier, car on peut toujours parvenir à un radical à indice quelconque par des extractions successives de racines à indices premiers; alors on doit avoir $r = 2$, puisque dans ce cas seulement on peut avoir $\alpha = -1$. *La première racine que l'on doit extraire est donc une racine carrée.* y est une fonction rationnelle de x_1, x_2, ..., x_n qui change de signe quand on échange x_1 et x_2, ou même quand on échange deux racines quelconques, car

on peut supposer, avant l'extraction de la racine carrée, que l'on ait mis dans A, à la place de x_1 et x_2, deux racines quelconques.

y n'est pas symétrique, mais il jouit d'une propriété caractéristique ; il reste invariable par une substitution circulaire effectuée entre un nombre impair de racines. Par exemple, quand on met x_1 à la place de x_2, x_2 à la place de x_3, x_3 à la place de x_1, cela revient en effet à faire un nombre pair d'échanges entre deux racines, ce qui chaque fois produit un changement de signe, et ce qui finalement reproduit la valeur initiale.

Si l'on continue à combiner le radical avec des radicaux analogues et avec les coefficients, qui sont des fonctions symétriques des racines, puis avec de nouveaux radicaux, et ainsi de suite, deux cas peuvent se présenter : ou bien les nouvelles expressions présenteront ce caractère de rester inaltérées par toutes les permutations circulaires de 3 et 5 racines, ou bien on finira par être obligé d'extraire une racine, et le résultat obtenu ne présentera plus le caractère en question. Dans le premier cas, on finira par trouver

$$x_1 = f(x_1, x_2, x_3, \ldots, x_n),$$

ce qui doit être une identité, ce qui est absurde si l'on a plus de deux racines, une permutation circulaire de trois lettres altérant le premier membre sans altérer le second, d'après notre hypothèse.

Il faut donc nécessairement que l'on tombe sur un radical qui ne présente plus le caractère en question. Ainsi on parviendra à une expression

$$z = \sqrt[r]{B},$$

dans laquelle B reste inaltéré après une permutation circulaire quelconque de 3 ou 5 racines, cette propriété n'appartenant pas à z.

Supposons que z change de valeur quand on remplace x_1, x_2, x_3 par x_2, x_3, x_1 respectivement, les valeurs de z sont

racines de

$$z^r = \mathrm{B};$$

entre deux valeurs de z, on aura une relation de la forme

$$f(x_1, x_2, x_3, x_4, \ldots, x_n) = \alpha f(x_2, x_3, x_1, x_4, \ldots, x_n),$$

qui doit être identique; elle doit donc subsister quand on y permute les trois racines. On a donc

$$f(x_2, x_3, x_1, x_4, \ldots, x_n) = \alpha f(x_3, x_1, x_2, x_4, \ldots, x_n),$$
$$f(x_3, x_1, x_2, x_4, \ldots, x_n) = \alpha f(x_1, x_2, x_3, x_4, \ldots, x_n)$$

et en multipliant les trois équations, membre à membre, on a

$$\alpha^3 = 1.$$

Si donc il y a trois ou un plus grand nombre de racines, on doit rencontrer un radical cubique.

Désignons par

$$z, \quad \alpha z, \quad \alpha^2 z$$

les trois valeurs de ce radical, on a

$$z^3 = \mathrm{B}.$$

Supposons qu'il y a plus de quatre racines; une permutation circulaire de cinq lettres n'altère pas B. Par cette permutation, pour que l'équation ne change pas, z doit se changer en αz ou en $\alpha^2 z$; si z change par cette permutation, on montrera comme tout à l'heure que

$$\alpha^5 = \pm 1,$$

ce qui est impossible, puisque α est une valeur imaginaire de $1^{\frac{1}{3}}$.

Alors z doit rester invariable par la permutation circulaire de cinq lettres : c'est la seule hypothèse qui nous reste à faire, en supposant qu'une substitution circulaire de trois racines le multiplie par α ou α^2.

Or, une permutation circulaire de trois quantités peut s'ob-

tenir en exécutant deux permutations de cinq d'entre elles. Ainsi une permutation circulaire de

$$x_1, \quad x_3, \quad x_2$$

peut s'obtenir en exécutant, par exemple, une substitution circulaire entre

$$x_5, \quad x_4, \quad x_3, \quad x_1, \quad x_2,$$

puis entre

$$x_1, \quad x_2, \quad x_3, \quad x_4, \quad x_5;$$

comme z doit rester invariable après une permutation de cinq lettres, elle doit aussi rester invariable après une permutation de trois lettres; ceci étant en contradiction avec nos hypothèses, il est prouvé que l'équation générale d'un degré supérieur au quatrième ne peut être résolue algébriquement ([1]).

([1]) Par ce mot *algébriquement*, il faut entendre que l'équation ne peut pas être résolue au moyen d'extraction de racines et des autres opérations algébriques. Abel et Galois ont aussi examiné la possibilité d'exprimer x_1 au moyen de formules algébriques ne se réduisant pas identiquement à x_1.

CHAPITRE V.

DÉCOMPOSITION DES POLYNOMES RATIONNELS EN FACTEURS RATIONNELS.

Facteurs du premier degré.

71. Les facteurs rationnels du premier degré d'un polynome rationnel $f(x)$ peuvent toujours être calculés. Un facteur de cette espèce doit en effet avoir la forme $x-\alpha$, et α doit être un facteur du terme indépendant de x; plus tard nous reviendrons sur cette question; nous remarquerons seulement ici qu'il n'y a à chercher que des facteurs $x-\alpha$ dans lesquels α divise le dernier terme; si de pareils facteurs n'existent pas, l'équation $f(x)=0$ n'a pas de racines rationnelles et $f(x)$ n'a pas de facteurs rationnels du premier degré.

Expression générale d'un facteur de $f(x)$.

72. Soit

$$f(x)=0 \tag{1}$$

l'équation générale du degré n sans racines égales. Soient

$$x_1, \quad x_2, \quad \ldots, \quad x_n$$

ses racines; soit

$$y_1=\varphi(x_1, x_2, \ldots, x_p) \tag{2}$$

une fonction rationnelle déterminée de p racines et

$$\varphi_1, \quad \varphi_2, \quad \ldots, \quad \varphi_r$$

les valeurs algébriques que l'on obtient en permutant dans φ toutes les racines de l'équation. Désignons par

$$y_1, \ y_2, \ \ldots, \ y_q$$

les valeurs numériques de celles d'entre elles où l'une des racines, x_1, par exemple, est restée à sa place. Les diverses valeurs de φ sont déterminées par une équation à coefficients rationnels. Soit y_1 une racine de cette équation et soit α son degré de multiplicité, alors

$$y_1 = \varphi_1 = \varphi_2 = \ldots = \varphi_\alpha;$$

considérons l'équation

$$(3) \qquad (y - y_1)(y - y_2)\ldots(y - y_q) = 0;$$

ses coefficients sont des fonctions symétriques des racines de

$$\frac{f(x)}{x - x_1} = 0$$

et peuvent s'exprimer rationnellement en fonction de x_1 et des quantités connues; et (3) pourra se mettre sous la forme

$$(4) \qquad F(y, x_1) = 0.$$

Puisque y_1 est racine de cette équation, on a

$$(5) \qquad F(y_1, x_1) = 0;$$

ce qui montre que x_1 est racine de

$$(6) \qquad F(y_1, x) = 0;$$

cette dernière a donc une racine commune avec la proposée.

Voyons si ces équations peuvent avoir d'autres racines communes, par exemple x_m. Pour cela il faut que

$$F(y_1, x_m) = 0,$$

ce qui exprime que y_1 est racine de

$$F(y, x_m) = 0.$$

Cette équation se déduit de (4) en changeant x_1 en x_m, ou, ce qui revient au même, elle s'obtient en faisant le même

changement dans (3) qui est identique à (4). Par ce changement $y_1, y_2 \ldots$ se changent dans des valeurs de φ, de sorte que la condition pour que x_m soit une racine commune consiste en ce qu'il existe une valeur φ_k de φ, dans laquelle x_m remplace x_1 et pour laquelle

$$y_1 = \varphi_k;$$

cette dernière équation est satisfaite pour

$$k = 1, \quad k = 2, \quad \ldots, \quad k = \alpha;$$

donc *les deux équations*

$$(7) \qquad f(x) = 0, \qquad F(y_1, x) = 0$$

ont pour racines communes toutes celles qui peuvent prendre la place de x_1 dans

$$(8) \qquad \varphi_1, \quad \varphi_2, \quad \ldots, \quad \varphi_\alpha.$$

On peut tirer diverses conséquences de ce théorème qui a été donné sous une forme un peu moins générale par Lagrange et par Galois.

73. *Dans le cas où l'équation en φ n'a pas de racines égales* on a seulement

$$y_1 = \varphi_1;$$

si donc φ est dissymétrique et d'une forme telle qu'*aucune racine ne puisse prendre la place de x_1 sans que la valeur algébrique de φ change*, x_1 reste alors la seule racine commune aux deux équations; elle peut alors s'exprimer rationnellement au moyen de y_1 et des quantités connues. En particulier, cela aura lieu pour toutes les racines de l'équation si

$$y = \varphi(x_1, x_2, \ldots, x_n)$$

prend des valeurs toutes différentes pour les $n!$ permutations des racines. C'est la forme donnée par Galois au théorème qui nous occupe.

Si φ est symétrique ou présente une symétrie partielle, toutes les racines qui peuvent prendre la place de x_1, sans changer la forme algébrique de φ_1, sont racines communes

aux deux équations. Considérons en particulier le cas où toutes les p racines peuvent être échangées dans φ_1, les deux équations ont p racines communes et, par la méthode du plus grand commun diviseur, *on peut former une équation qui détermine ces racines communes, ou le facteur du $p^{\text{ième}}$ degré correspondant de $f(x)$.*

La forme la plus générale d'un facteur du $p^{\text{ième}}$ degré de $f(x)$ est alors

$$(9) \qquad x^p + \varphi_1(y_1)x^{p-1} + \varphi_2(y_1)x^{p-2} \ldots + \varphi_p(y_1) \ldots,$$

où $\varphi_1, \varphi_2, \ldots, \varphi_p$ sont des fonctions rationnelles de y_1 et des quantités connues, y_1 désignant la valeur d'une fonction symétrique de p racines qui est déterminée par une équation dont toutes les racines sont simples. On peut ainsi dans ce cas exprimer toutes les fonctions symétriques des p racines en fonction d'une d'entre elles et des quantités connues.

Exemple I. — Pour l'équation

$$x^3 - 6x^2 + 11x - 6 = 0,$$

si l'on donne

$$x_1^2 + x_2^2 = 5;$$

on posera

$$y_1 = x_1^2 + x_2^2, \qquad y_2 = x_1^2 + x_3^2$$

et l'on obtiendra, en éliminant x_2 et x_3,

$$y^2 - (x_1^2 + 14)y + 14x_1^2 + \frac{36}{x_1^2} = 0;$$

ou, en remplaçant x_1 par x et y par 5,

$$x^4 - 5x^2 + 2 = 0,$$

équation qui a avec la proposée les racines de

$$x^2 - 3x + 2 = 0.$$

Exemple II. — Trouver la forme générale des diviseurs du second degré de

$$f(x) = x^3 + ax^2 + bx + c$$

en fonction du produit y de deux racines de $f(x) = 0$

$$y_1 = x_1 x_2, \qquad y_2 = x_1 x_3,$$
$$x_2 + x_3 = -a - x_1;$$

ainsi

$$y^2 + (x_1^2 + a x_1) y - x_1 c = 0,$$

d'où la forme cherchée

$$x^2 + \frac{ay - c}{y} x + y.$$

74. L'équation en φ qui a $n!$ racines inégales et dont nous avons fait usage plus haut appartient à une classe remarquable d'équations dont nous allons nous occuper. Elles ont cette propriété *que chaque racine peut s'exprimer rationnellement en fonction de chacune des autres.* En effet, chaque racine est fonction rationnelle de $x_1, x_2, \ldots, x_n$ qui, à leur tour, sont fonctions rationnelles d'une des valeurs de φ.

On peut utiliser cette propriété pour *exprimer autant d'irrationnelles que l'on veut rationnellement, au moyen d'une même irrationnelle, en appelant irrationnelle une racine d'une équation algébrique à coefficients rationnels; peu importe d'ailleurs que l'on puisse ou non exprimer cette irrationnelle au moyen de radicaux.*

En effet, soient $x_1, x_2, \ldots, x_p$ des irrationnelles, déterminées par diverses équations algébriques dont elles sont racines. On peut toujours (par exemple au moyen d'une simple multiplication) former une équation dont ces quantités soient racines; si l'on considère une fonction des racines de cette équation dont toutes les valeurs, obtenues en permutant les racines, soient distinctes, les racines de cette équation et les irrationnelles données seront exprimables rationnellement au moyen de cette fonction. On peut, par exemple, prendre cette fonction égale à

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n, \tag{10}$$

en supposant l'équation auxiliaire de degré n. Il est évident que l'on peut choisir les coefficients $\alpha_1, \alpha_2, \ldots, \alpha_n$

puisque $x_1, x_2, \ldots$ sont différents, de telle sorte que toutes les valeurs de y soient distinctes.

75. Supposons toujours l'équation donnée de degré n et les $n!$ valeurs de φ distinctes, l'équation en φ pourra être réductible; dans ce cas, supposons-la décomposée en équations irréductibles; soient

$$(11) \qquad \varphi_1, \quad \varphi_2, \quad \ldots, \quad \varphi_p$$

les racines de l'une d'elles. On peut, comme on l'a vu, exprimer chaque racine de l'équation donnée en fonction rationnelle d'une valeur de φ, en sorte que les racines pourront être représentées par

$$(12) \qquad \Psi_1(\varphi_1), \quad \Psi_2(\varphi_1), \quad \ldots, \quad \Psi_n(\varphi_1).$$

Si dans cette suite on remplace φ_1 *par un autre terme de la série* (11), *la nouvelle suite représentera encore les racines de l'équation donnée, mais dans un autre ordre.*

Pour trouver l'une des racines, x_1, par exemple, posons

$$y_1 = \varphi_1;$$

si dans φ_1 on intervertit l'ordre des racines, on peut transformer un autre terme de (11); le calcul, dans les deux cas, sera le même, à l'ordre près des racines, et si l'on a

$$x_1 = \Psi_1(\varphi_1),$$

on aura

$$x_p = \Psi_1(\varphi_p),$$

x_p désignant la racine échangée avec x_1, quand φ_p remplace φ_1. Les nouvelles valeurs sont distinctes; car si l'on avait, par exemple,

$$\Psi_1(\varphi_p) = \Psi_2(\varphi_p),$$

φ_p serait une racine commune à $\Psi_1(\varphi) - \Psi_2(\varphi) = 0$ et à l'équation irréductible qui a pour racines les quantités (11).

On devrait donc aussi avoir $\Psi_1(\varphi_1) - \Psi_2(\varphi_1) = 0$ (13), ce qui est absurde puisque les quantités (12) sont distinctes.

Nous verrons plus loin que ce théorème est fondamental dans les applications de la théorie des substitutions à la théorie des équations.

76. Des développements qui précèdent, il résulte que dans le cas où $f(x)$ a des facteurs rationnels, il est toujours possible de les trouver. Par exemple, si $f(x)$ possède un facteur rationnel de degré p, il devra exister p racines de $f(x) = 0$ dont le produit est rationnel. On peut trouver ce produit y en formant l'équation qui a pour racines les produits de p racines de la proposée, cette équation a alors une racine rationnelle; appelons-la k. On aura

$$x_1 x_2 \ldots x_p = k,$$

et les coefficients du facteur rationnel peuvent être exprimés en fonctions rationnelles de k. Si l'équation en y avait des racines égales, on pourrait partir d'une autre fonction symétrique des racines, par exemple

$$y = (\alpha - x_1)(\alpha - x_2) \ldots (\alpha - x_p),$$

où l'on peut toujours choisir α de telle sorte que l'équation en y n'ait pas de racines égales, si la proposée elle-même n'en a pas. Comme k est facteur du dernier terme de l'équation, on peut, quand il n'a pas un grand nombre de facteurs, au moyen de tâtonnements, simplifier la recherche de l'équation qui donne k.

Quand k est rationnel, il existe un facteur rationnel, pourvu que k ne soit pas racine multiple; en effet, si k était racine multiple, il n'existe pas nécessairement un facteur rationnel de degré p, car les équations (7), dans ce cas, peuvent avoir un facteur commun de degré plus élevé. Nous reviendrons sur ce cas un peu plus tard; nous nous bornerons à observer ici que *si une équation est réductible, il est toujours possible de la décomposer en d'autres irréductibles.*

CHAPITRE VI.

ÉQUATIONS ABÉLIENNES.

Équations dans lesquelles une racine peut s'exprimer rationnellement en fonction d'une autre.

77. Gauss a montré que les équations qui servent à partager la circonférence en parties égales sont résolubles algébriquement; ces équations sont comprises dans une classe d'équations, étudiées plus tard par Abel et qui portent le nom d'*équations abéliennes;* ce sont des équations dans lesquelles une racine peut s'exprimer rationnellement en fonction d'une autre. Les équations réciproques et les équations du 3e degré, par exemple, appartiennent à cette classe (Exercice 54). Les équations abéliennes peuvent toujours être abaissées et souvent même résolues algébriquement.

Nous supposerons que, dans l'équation irréductible de degré n,

$$f(x) = 0, \tag{1}$$

on ait entre deux racines la relation

$$x_1 = \theta(x_2), \tag{2}$$

où θ désigne une fonction rationnelle.

Si l'on forme l'équation en y qui a pour racines

$$y_1 = \theta(x_1),\quad y_2 = \theta(x_2),\quad \ldots,\quad y_n = \theta(x_n), \tag{3}$$

on obtient une équation qui a une racine commune avec la proposée et, comme celle-ci est irréductible, les deux équa-

tions en x et en y étant de même degré doivent avoir les mêmes racines. Il en résulte que, si l'on exécute l'opération θ sur une racine quelconque, on doit en trouver une autre; si l'on opère sur celle-ci comme sur la première on en trouve une troisième, et ainsi de suite, jusqu'à ce que l'on retombe sur une racine déjà obtenue. Un groupe de racines, par exemple trois, sera donc lié par des équations telles que

$$(4) \qquad \begin{cases} x_1 = \theta(x_2), \\ x_2 = \theta(x_3), \\ x_3 = \theta(x_1); \end{cases}$$

si l'on désigne alors $\theta[\theta(x)]$ par $\theta^2(x)$, etc., ces équations donnent

$$(5) \qquad x_1 = \theta^3(x_1);$$

cette équation ne saurait être identique si l'on suppose à θ la forme entière, ce qui est possible (26), et si l'on exclut le cas où θ serait linéaire; cette équation $x - \theta^3(x) = 0$ a une racine x_1 commune avec $f(x) = 0$, elle admet donc toutes les racines de cette équation. Si en dehors des racines x_1, x_2, x_3 on prend une racine x_4, celle-ci doit donc former un groupe avec deux autres racines; dans ce groupe il ne peut entrer plus de trois racines, car l'équation $x_4 = \theta^3(x_4)$ montre qu'après avoir effectué trois fois l'opération θ on doit retrouver x_4; il ne peut pas entrer moins de trois racines dans le groupe, car si l'on avait $x_4 = \theta^2(x_4)$ on aurait aussi $x_1 = \theta^2(x_1)$ et le premier groupe ne contiendrait que deux racines. La même racine ne peut entrer dans deux groupes différents, car si le second groupe contenait x_4, x_5 et x_1 on aurait

$$\theta(x_1) = x_3, \qquad \theta(x_1) = x_5$$

et $x_3 = x_5$, ce qui est absurde, l'équation proposée n'ayant pas de racines égales.

On voit ainsi que *les racines se partagent en groupes contenant le même nombre de racines, et si n est premier, il n'y aura qu'un groupe.* Si n est un nombre composé il doit être divisible par le nombre des racines de chaque groupe.

Si, par exemple, on a m groupes de p racines, $n = mp$. L'équation peut alors se résoudre à l'aide d'une équation de degré p dont les coefficients dépendent d'une équation de degré m.

Si, pour plus de simplicité, nous supposons p toujours égal à 3, on peut poser

$$(6) \qquad y_1 = x_1 + x_2 + x_3 = \theta^2(x_3) + \theta(x_3) + x_3,$$

si l'on remplace x_3 par toutes les racines de l'équation proposée, on obtiendra $3m$ valeurs pour y_1.

Ces valeurs sont égales trois à trois; ainsi

$$\theta^2(x_2) + \theta(x_2) + x_2 = x_3 + x_1 + x_2,$$
$$\theta^2(x_1) + \theta(x_1) + x_1 = x_2 + x_3 + x_1;$$

y n'a ainsi que m valeurs et sera fourni par une équation de degré m à coefficients rationnels, que l'on obtiendra par la théorie des fonctions symétriques ou en éliminant x entre

$$(7) \qquad f(x) = 0 \quad \text{et} \quad y = x + \theta(x) + \theta^2(x);$$

la résultante

$$(8) \qquad \varphi(y) = 0$$

du degré m a pour racines

$$(9) \qquad \begin{cases} y_1 = x_1 + x_2 + x_3, \\ y_2 = x_4 + x_5 + x_6, \\ \dots\dots\dots\dots\dots\dots, \\ y_m = x_{3m-2} + x_{3m-1} + x_{3m}; \end{cases}$$

dans le cas où ces racines sont inégales, on peut trouver la forme générale d'un diviseur du 3e degré de $f(x)$

$$x^3 - y_p x^2 + \Psi_1(y_p)x + \Psi_2(y_p);$$

si l'on remplace y_p successivement par $y_1, y_2, \dots, y_m$, on obtient les m facteurs du 3e degré de $f(x)$; de telle sorte que l'équation donnée du degré $3m$ est réduite aux équations

$$(10) \qquad \begin{cases} x^3 - y x^2 + \Psi_1(y)x + \Psi_2(y) = 0, \\ \varphi(y) = 0; \end{cases}$$

la première est du troisième degré et la seconde du $m^{\text{ième}}$ degré. Les mêmes considérations sont applicables au cas où le groupe contiendrait, au lieu de trois, un nombre quelconque de racines.

L'équation $\varphi(y) = 0$ ne donne pas lieu à l'examen de cas particuliers : elle peut être quelconque ; l'autre est encore une équation abélienne, car ses racines forment encore un groupe doué des propriétés considérées plus haut. Nous verrons plus loin qu'elle est toujours résoluble algébriquement.

78. $\varphi(y) = 0$ peut avoir des racines égales; alors on peut partir de la fonction

$$(11) \quad y_1 = (\alpha - x_1)(\alpha - x_2)(\alpha - x_3) = [\alpha - \theta^2(x_3)][\alpha - \theta(x_3)](\alpha - x_3),$$

où α peut être choisi de telle sorte que deux valeurs de y_1 ne puissent être égales. Si l'on avait, en effet, pour toute valeur de α, $y_1 = y_2$ par exemple, ou

$$(\alpha - x_1)(\alpha - x_2)(\alpha - x_3) = (\alpha - x_4)(\alpha - x_5)(\alpha - x_6),$$

les trois racines du premier groupe seraient égales à celles du second, et l'équation donnée serait réductible.

Le résultat de cette discussion est donc que ;

Si p des racines d'une équation irréductible peuvent se mettre sous la forme x_1, $\theta(x_1)$, $\theta^2(x_1)$, ..., $\theta^{p-1}(x_1)$, où θ est tel que $\theta^p(x_1) = x_1$, cette équation est de degré mp et elle peut, à l'aide d'une équation de degré m, être réduite à une autre de degré p.

Équations abéliennes dont les racines forment un groupe.

79. Il reste à étudier l'équation du degré n

$$(1) \qquad f(x) = 0,$$

dont les racines peuvent être mises sous la forme

$$(2) \qquad x_1, \quad \theta(x_1), \quad \theta^2(x_1), \quad \ldots, \quad \theta^{n-1}(x_1),$$

où x_1 désigne une racine quelconque et où

$$(3) \qquad \theta^n(x_1) = x_1.$$

Désignons par α une racine quelconque de

$$(4) \qquad x^n = 1;$$

l'expression

$$(5) \quad \Psi(x_1) = [x_1 + \alpha\theta(x_1) + \alpha^2\theta^2(x_1) + \ldots + \alpha^{n-1}\theta^{n-1}(x_1)]^n,$$

où α est considéré comme connu, n'a qu'une seule valeur et, par suite, peut s'exprimer rationnellement en fonction des coefficients de l'équation donnée des coefficients de θ et de α.

Si l'on prend, au lieu de x_1, une autre racine, par exemple $x_3 = \theta^2(x_1)$, on a

$$\Psi(x_3) = [\theta^2(x_1) + \alpha\theta^3(x_1) + \alpha^2\theta^4(x_1) + \ldots + \alpha^{n-1}\theta(x_1)]^n,$$

où la quantité entre crochets se déduit de celle qui est analogue dans (5) en la multipliant par α^{n-2}. Comme $\alpha^n = 1$, les deux expressions de $\Psi(x_1)$ et de $\Psi(x_3)$ sont égales. On voit ainsi que

$$(6) \qquad \Psi(x_1) = \Psi(x_2) = \ldots = \Psi(x_n).$$

On peut poser

$$(7) \qquad \Psi(x_1) = \frac{1}{n}[\Psi(x_1) + \Psi(x_2) + \ldots + \Psi(x_n)]$$

et calculer Ψ comme une fonction symétrique. Elle contient α et, par suite, possède une valeur pour chaque valeur de α.

Si l'on appelle υ_r la valeur de Ψ qui correspond à la valeur α_r de α, on obtient n équations de la forme

$$(8) \qquad x + \alpha_r\theta(x) + \alpha_r^2\theta^2(x) + \ldots + \alpha_r^{n-1}\theta^{n-1}(x) = \sqrt[n]{\upsilon_r}.$$

La valeur correspondant à $\alpha_r = 1$ de $\sqrt[n]{\upsilon_r}$ est connue, car on connaît la somme des racines, elle est $-$A, si A est le coefficient de x^{n-1}. Si l'on ajoute les n équations (8), et si l'on observe que

$$\Sigma\alpha^p = 0,$$

pour toutes les valeurs de p non divisibles par n, on trouve, en supposant $\alpha_0 = 1$,

$$(9) \qquad x = \frac{-A + \sqrt[n]{\upsilon_1} + \sqrt[n]{\upsilon_2} + \ldots + \sqrt[n]{\upsilon_{n-1}}}{n}.$$

Si l'on multiplie chaque équation par α_r^{-m} avant de les ajouter, tous les termes du premier membre s'annulent, excepté $\theta^m(x)$, et l'on obtient une quelconque des racines par la formule

$$(10) \qquad \theta^m(x) = \frac{-A + \alpha_1^{-m}\sqrt[n]{\upsilon_1} + \alpha_2^{-m}\sqrt[n]{\upsilon_2} + \ldots + \alpha_{n-1}^{-m}\sqrt[n]{\upsilon_{n-1}}}{n}.$$

Dans cette expression, on peut prendre un des radicaux, avec une quelconque de ses valeurs, mais alors les valeurs des autres doivent s'en déduire. Par exemple si, dans l'expression de υ_1, α désigne une racine primitive de l'unité, les autres valeurs de α seront ses puissances $\alpha_p = \alpha^p$, et l'on a

$$(11) \qquad \begin{cases} \sqrt[n]{\upsilon_1} = x + \alpha\theta(x) + \alpha^2\theta^2(x) + \ldots + \alpha^{n-1}\theta^{n-1}(x), \\ \sqrt[n]{\upsilon_p} = x + \alpha^p\theta(x) + \alpha^{2p}\theta^2(x) + \ldots + \alpha^{(n-1)p}\theta^{n-1}(x); \end{cases}$$

si l'on change, dans ces deux équations, x en $\theta^m(x)$, la première se trouve multipliée par α^{-m}, la seconde par α^{-pm}. Le produit

$$(12) \qquad \varphi(x) = \left(\sqrt[n]{\upsilon_1}\right)^{n-p}\sqrt[n]{\upsilon_p}$$

se trouve alors multiplié par

$$\alpha^{-m(n-p)}\alpha^{-mp} = \alpha^{-mn} = 1;$$

il se trouve donc inaltéré quand on y permute deux valeurs de x; $\varphi(x)$ est donc une fonction rationnelle qui peut être calculée comme plus haut $\Psi(x)$. Si l'on désigne sa valeur par a_p, on a

$$(13) \qquad \sqrt[n]{\upsilon_p} = \frac{a_p}{\upsilon_1}\left(\sqrt[n]{\upsilon_1}\right)^p.$$

Tous les radicaux qui entrent dans la valeur de x peuvent donc s'exprimer rationnellement en fonction de l'un d'entre

eux; si l'on remplace ces radicaux par leurs valeurs dans (9), on obtient pour x une expression qui n'a que n valeurs correspondant aux valeurs de $\sqrt[n]{\upsilon_1}$. α entre dans le résultat, et nous verrons plus loin qu'on peut l'exprimer algébriquement. On voit ainsi qu'*une équation dont les racines peuvent être représentées par* x, $\theta(x)$, $\theta^2(x)$, $\ldots$, $\theta^{n-1}(x)$, *où* $\theta^n(x)=x$, *est résoluble algébriquement.*

Comme cela a toujours lieu quand n est premier, dès qu'une racine est fonction rationnelle d'une autre, *une équation de degré premier dont une racine est fonction rationnelle d'une autre, et qui est irréductible, est résoluble algébriquement.*

Dans le cas où les fonctions f et θ sont à coefficients réels, α sera la seule imaginaire contenue dans υ_1 et, comme les valeurs de α sont conjuguées deux à deux, à savoir α^k et α^{n-k}, il doit en être de même pour les valeurs de υ; ainsi

$$(14)\qquad \begin{cases} \upsilon_1 \phantom{{}_{n-1}} = \rho(\cos\omega + i\sin\omega), \\ \upsilon_{n-1} = \rho(\cos\omega - i\sin\omega), \end{cases}$$

où (12)

$$(15)\qquad \rho^2 = \upsilon_1\upsilon_{n-1} = a_{n-1}^n.$$

Comme $a_{n-1} = \sqrt[n]{\upsilon_1}\sqrt[n]{\upsilon_{n-1}}$ quand on échange α et α^{n-1} reste inaltéré et ne contient d'autre imaginaire que α, il doit être réel. On a donc

$$(16)\qquad \sqrt[n]{\upsilon_1} = \sqrt{a}\left(\cos\frac{2p\pi+\omega}{n} + i\sin\frac{2p\pi+\omega}{n}\right),$$

où a désigne la valeur numérique de a_{n-1}; il en résulte

$$(17)\qquad \sqrt[n]{\upsilon_k} = \frac{a_k}{\upsilon_1}\sqrt{a^k}\left[\cos\frac{k(2p\pi+\omega)}{n} + i\sin\frac{k(2p\pi+\omega)}{n}\right].$$

De sorte que les racines ne dépendent que de quantités rationnelles, d'une racine carrée, du sinus et du cosinus de la $n^{\text{ième}}$ partie de la circonférence, et de la même partie d'un angle ω dont la tangente est fonction rationnelle du sinus et du cosinus de ce même angle ω.

Comme θ est réel, on voit immédiatement que les racines

sont toutes réelles ou toutes imaginaires, car si l'une est réelle, les autres le sont aussi.

Examen du cas où le degré de l'équation n'est pas un nombre premier.

80. La méthode que nous avons fait connaître pour la résolution des équations abéliennes dont les racines forment un groupe, est tout à fait générale ; mais, quand le degré n'est pas un nombre premier, la solution peut être simplifiée.

Soit $n = pm$; on peut répartir les racines en groupes de p racines, à savoir :

$$(1)\quad \left\{\begin{array}{lllll} x, & \theta^m(x), & \theta^{2m}(x), & \ldots, & \theta^{(p-1)m}(x), \\ \theta(x), & \theta^{m+1}(x), & \theta^{2m+1}(x), & \ldots, & \theta^{(p-1)m+1}(x), \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots\ldots, \\ \theta^{m-1}(x), & \theta^{2m-1}(x), & \ldots, & \theta^{pm-1}(x), & \end{array}\right.$$

et l'on pose alors

$$(2)\qquad \theta^m(x) = \theta_1(x),$$

les racines placées sur la première ligne seront

$$(3)\qquad x,\quad \theta_1(x),\quad \theta_1^2(x),\quad \ldots,\quad \theta_1^{p-1}(x),$$

ou

$$(4)\qquad \theta_1^p(x) = \theta^{mp}(x) = x.$$

On peut donc, d'après ce que l'on a vu (77), réduire l'équation, à l'aide d'une équation de degré m, à une autre de degré p. L'équation de degré p a la même propriété que la proposée; cela n'a pas lieu pour l'équation de degré m dans le cas traité (77) et (78). Mais on peut montrer que, ici, où toutes les racines forment un groupe, les deux équations auxquelles se réduisent la proposée jouissent de la même propriété.

L'équation du degré m en y est constituée de telle sorte que l'une de ses racines est fonction symétrique des p racines

du premier groupe; les autres dépendent de la même façon des racines des autres groupes.

Soit maintenant y_1 la racine qui peut s'exprimer au moyen de

(5) $$x,\quad \theta^m(x),\quad \theta^{2m}(x),\quad \ldots,\quad \theta^{(p-1)m}(x),$$

soit y_2 celle qui peut s'exprimer au moyen de

(6) $$\theta(x),\quad \theta^{m+1}(x),\quad \ldots,\quad \theta^{(p-1)m+1}(x),$$

les coefficients de l'équation qui a pour racines les quantités (5) sont fonctions rationnelles de y_1, et toutes les fonctions symétriques des racines peuvent s'exprimer rationnellement en y_1; y_2 est une fonction symétrique de

$$\theta(x),\quad \theta\theta^m(x),\quad \theta\theta^{2m}(x),\quad \ldots,$$

et, par conséquent, aussi des racines (5); y_2 peut donc s'exprimer rationnellement en y_1, de sorte que l'équation en y jouit de la même propriété que la proposée.

Si m et p sont des nombres composés, on peut continuer de la même façon, et *toute équation abélienne dont les racines forment un groupe peut être ramenée à des équations abéliennes de degré premier.*

Sur les équations irréductibles dont deux racines sont liées par la relation

(1) $$x_1 x_2 + a x_1 + b x_2 + c = 0.$$

81. Nous supposerons que a, b et c sont des fonctions rationnelles de quantités dont les coefficients de l'équation sont eux-mêmes des fonctions rationnelles. Si l'on change dans l'équation x en $x+h$, h étant déterminé par l'équation

(2) $$h^2 + (a+b)h + c = 0,$$

deux racines seront liées par la relation

(3) $$x_1 x_2 + (h+a)x_1 + (h+b)x_2 = 0;$$

si l'on change ensuite x en $\frac{1}{x}$, on obtient entre deux racines la nouvelle relation

$$(4) \qquad 1 + (h + a)x_2 + (h + b)x_1 = 0;$$

si enfin on change x en $x + h_1$ ou

$$(5) \qquad (2h + b + a)h_1 + 1 = 0,$$

on obtient une équation dans laquelle deux racines sont liées par la relation

$$(6) \qquad x_1 = \alpha x_2, \qquad \text{où} \qquad \alpha = -\frac{h + a}{h + b}.$$

Maintenant supposons que l'équation donnée continue à être irréductible, même lorsque l'on regarde h comme une quantité connue, bien qu'il soit donné par une équation du second degré, quantité pouvant être utilisée dans la décomposition en facteurs; dans ce cas, l'équation finale doit être considérée comme irréductible; car, si elle pouvait se décomposer en plusieurs autres, il suffirait, pour décomposer l'équation primitive, de revenir aux inconnues primitives. Un groupe de racines sera donné par les relations

$$(7) \qquad x_1 = \alpha x_2, \qquad x_2 = \alpha x_3, \qquad \ldots, \qquad x_p = \alpha x_1,$$

qui montrent que α est racine primitive de

$$(8) \qquad \alpha^p = 1.$$

De

$$(9) \qquad \alpha = -\frac{h + a}{h + b},$$

on tire

$$(10) \qquad h = -\frac{a + b\alpha}{1 + \alpha};$$

et alors, en remplaçant h par cette valeur dans (2), on a

$$(11) \qquad \alpha^2(ab - c) + (a^2 + b^2 - 2c)\alpha + ab - c = 0.$$

L'une des racines de cette équation est l'imaginaire conju-

guée de α, car le produit des racines est un; soient

$$\cos\upsilon + i\sin\upsilon$$

et

$$\cos\upsilon - i\sin\upsilon$$

ces racines; on a

$$2\cos\upsilon = \frac{a^2+b^2-2c}{c-ab} = \frac{(a-b)^2}{c-ab} - 2,$$

ou

(12) $$c = ab + \frac{(a-b)^2}{4\cos^2\frac{\mu\pi}{p}}; \qquad h = -\frac{a+b}{2} \pm i\,\frac{a-b}{2}\,\text{tang}\,\frac{\mu\pi}{p},$$

où μ est premier avec p, puisque α est une racine primitive.

On voit qu'un groupe de p racines de l'équation transformée peut être exprimé au moyen de l'une d'entre elles; si l'on désigne par y_1 cette racine, les p racines sont données par l'équation

$$x^p - y_1^p = 0,$$

et s'il y a m semblables groupes, on pourra mettre l'équation transformée sous la forme

(13) $$(x^p - y_1^p)(x^p - y_2^p)\ldots(x^p - y_m^p) = 0;$$

$y_1^p, y_2^p, \ldots, y_m^p$ peuvent ainsi être considérés comme racines d'une équation quelconque du degré m. Soit

(14) $$f(y) = 0$$

cette équation, l'équation en x sera

(15) $$f(x^p) = 0,$$

et l'équation proposée doit être telle qu'on puisse la ramener à cette forme au moyen des transformations dont il a été question; on voit que p peut être supposé premier, sans diminuer la généralité de la solution.

82. Les équations, qui ont la forme générale que nous avons considérée, supposent que α puisse entrer dans la rela-

tion (1). Si cette relation ne contient que des quantités rationnelles,

$$\cos^2 \frac{\mu\pi}{p}$$

doit être rationnel et le nombre premier p doit être égal à 2 ou à 3.

Si $p = 2$, la valeur de c est illusoire ; dans ce cas

$$\alpha = -1 = -\frac{h+a}{h+b},$$

ainsi

$$a = b,$$

d'où la relation

$$(16) \qquad x_1 x_2 + a(x_1 + x_2) + c = 0.$$

Si l'on pose

$$y = x_1 + x_2,$$

on trouve l'équation en y en éliminant x entre la proposée et

$$x^2 - yx - ay - c = 0.$$

On reconnaît que l'équation appartient à cette classe, quand elle reste inaltérée en changeant x en

$$-\frac{ax+c}{x+a}.$$

Réciproquement on trouve toutes les équations du degré $2n$, qui appartiennent à cette classe, quand, dans l'équation générale du degré n en y, on pose

$$(17) \qquad y = \frac{x^2 - c}{x + a}.$$

Pour $p = 3$, on a

$$(18) \qquad c = ab + (a-b)^2,$$

et la relation

$$(19) \qquad x_1 x_2 + ax_1 + bx_2 + ab + (a-b)^2 = 0.$$

Ces équations doivent rester inaltérées quand on change x en

$$(20) \qquad -\frac{ax+a^2-ab+b^2}{x+b}.$$

Elles se réduisent à la forme

$$x'^3 = y,$$

où

$$(21) \quad x' = \frac{1}{x-h} + \frac{1}{2h+a+b}, \qquad x = h + \frac{2h+(a+b)}{(2h+a+b)x'-1},$$

et

$$(22) \qquad h = -\frac{a+b}{2} \pm \frac{a-b}{2}\sqrt{-3} = -a-(a-b)\alpha.$$

On peut facilement exprimer les coefficients de l'équation du troisième degré au moyen de l'un d'entre eux; si l'on pose

$$x_1+x_2+x_3=-y; \qquad x_1x_2+x_1x_3+x_2x_3=a_2;$$
$$x_1x_2x_3=-a_3,$$

on tire de

$$x_1x_2+ax_1+bx_2+a^2-ab+b^2=0,$$
$$x_2x_3+ax_2+bx_3+a^2-ab+b^2=0,$$
$$x_3x_1+ax_3+bx_1+a^2-ab+b^2=0,$$

en les ajoutant,

$$a_2-(a+b)y+3(a^2-ab+b^2)=0;$$

et en les ajoutant, après les avoir multipliées par x_3, x_1 et x_2,

$$-3a_3+(a+b)a_2-y(a^2-ab+b^2)=0;$$

d'où l'on déduit l'équation

$$(23) \quad x^3+yx^2+[(a+b)y-3(a^2-ab+b^2)]x+aby-(a^3+b^3)=0.$$

En éliminant y entre cette équation et

$$(24) \qquad F(y)=0,$$

où $F(y)=0$ est une équation irréductible arbitraire, on obtient une équation de l'espèce cherchée.

Exemple :

$$x^3 + x^2 - 2x - 1 = 0;$$

cette équation reste inaltérée quand on change x en $-\frac{1}{1+x}$; on a alors

$$x_1 x_2 + x_1 + 1 = 0;$$

ainsi

$$a = 1; \qquad b = 0; \qquad h = \alpha; \qquad h_1 = -\frac{1}{1+2\alpha} = \frac{1+2\alpha}{3};$$

l'équation réduite est

$$x'^3 = \frac{\pm 13\sqrt{-3} - 9}{126}.$$

83. Nous avons supposé que l'équation donnée reste irréductible quand la racine carrée qui entre dans h est censée connue; soit k cette racine, il peut arriver que l'équation se décompose en deux autres

$$A + kB = 0$$

et

$$A - kB = 0,$$

et alors il est clair que dans ce cas la relation (1) détermine x_2 comme racine d'une de ces deux équations quand x_1 est pris pour une autre racine.

L'équation transformée se laisse décomposer aussi en deux autres et chacune des racines de celles-ci x_k est déterminée en fonction d'une autre racine x_1 au moyen d'une relation de la forme

$$x_k = \alpha x_1;$$

on arrive donc à la même détermination de α que dans le cas général, de sorte que l'on peut énoncer le théorème suivant :

Si deux racines d'une équation irréductible du $n^{\text{ième}}$ degré sont liées par la relation (1), *l'équation peut être résolue au moyen d'une équation du second degré à l'aide d'une équation de degré $\frac{n}{2}$, dans le cas où $a = b$; dans le cas contraire, on peut la ramener à une équation du troisième degré, à*

l'aide d'une équation de degré $\frac{n}{3}$; dans ce dernier cas on doit avoir $c = a^2 - ab + b^2$.

84. Lorsque deux racines d'une équation irréductible, développées en fraction continue, finissent par avoir les mêmes quotients complets, l'équation appartient à la classe d'équations que nous venons d'étudier. Si le quotient complet commun est désigné par q on a

$$(25) \qquad x_1 = \frac{d + d_1 q}{e + e_1 q}, \qquad x_2 = \frac{f + f_1 q}{g + g_1 q},$$

$\frac{d}{e}$ et $\frac{d_1}{e_1}$ étant les dernières réduites de x_1 et $\frac{f}{g}$, $\frac{f_1}{g_1}$ étant les dernières réduites de x_2 que l'on obtient quand on fait usage des parties différentes des fractions continues. Si l'on élimine q on a

$$(26) \quad (eg_1 - ge_1)x_1 x_2 + (e_1 f - ef_1)x_1 + (d_1 g - dg_1)x_2 + df_1 - d_1 f = 0;$$

on a identiquement

$$(27) \quad \left\{ \begin{aligned} &(e_1 f - ef_1)(d_1 g - dg_1) + (de_1 - ed_1)(fg_1 - gf_1) \\ &\qquad\qquad = (eg_1 - ge_1)(df_1 - fd_1), \end{aligned} \right.$$

où, comme l'on sait,

$$(28) \quad \left\{ \begin{aligned} de_1 - de_1 &= \pm 1, \\ fg_1 - gf_1 &= \pm 1. \end{aligned} \right.$$

Pour $p = 2$, $(a = b)$, et si l'on pose

$$eg_1 - ge_1 = \lambda, \qquad e_1 f - ef_1 = d_1 g - g_1 d = a,$$

(27) donne

$$df_1 - d_1 f = \frac{a^2 \pm 1}{\lambda},$$

où λ est un diviseur de $a^2 \pm 1$; la forme générale d'une équation aux racines x_1 et x_2 est donc

$$(29) \qquad x^2 - xy - \frac{ay}{\lambda} - \frac{a^2 \pm 1}{\lambda^2} = 0,$$

où a désigne un entier quelconque, λ un diviseur de $a^2 \pm 1$

et y une racine d'une équation arbitraire. Pour $p=3$ en posant

$$e_1 f - f e_1 = a, \qquad d_1 g - g_1 d = b, \qquad \text{et} \qquad d f_1 - f d_1 = c,$$

(27) donne

$$ab \pm 1 = \lambda c$$

et l'on a (18)

$$\lambda c = a^2 - ab + b^2;$$

il en résulte

$$(b-a)^2 = \pm 1,$$

de sorte que l'on doit faire usage du signe $+$; on a donc

$$b = a \pm 1,$$
$$c = \frac{a^2 \pm a + 1}{\lambda}.$$

La forme la plus générale d'une équation du troisième degré aux racines x_1 et x_2 est donc

$$(30) \quad \begin{cases} x^3 + y x^2 + a_2 x + a_3 = 0, \\ \text{où} \\ a_2 = \dfrac{2a \pm 1}{\lambda} y - \dfrac{3(a^2 \pm a + 1)}{\lambda^2}, \\ a_3 = \dfrac{a^2 \pm a}{\lambda^2} - \dfrac{(2a \pm 1)(a^2 \pm a + 1)}{\lambda^3}; \end{cases}$$

a est un entier arbitraire et λ un diviseur de $a^2 \pm a + 1$.

Résolution algébrique des équations binomes.

85. On a montré que la résolution de l'équation binome se ramenait à la résolution d'équations de la forme

$$(1) \qquad x^p - 1 = 0,$$

où p désigne un nombre premier; les racines de cette équation ont été mises sous forme trigonométrique, et nous allons montrer maintenant comment on peut les mettre sous forme

algébrique. La somme de deux racines de l'équation (1) étant égale à $2\cos\frac{2\pi}{p}$, la circonférence pourra être partagée en p parties égales au moyen de la règle et du compas, si l'équation en question peut être résolue au moyen seulement de racines carrées.

Si l'on divise par $x-1$, on obtient l'équation irréductible

$$x^{p-1}+x^{p-2}+\ldots+x^2+x+1=0. \tag{2}$$

Les racines de cette équation peuvent être représentées au moyen de l'une d'elles α par les expressions

$$\alpha,\quad \alpha^{r},\quad \alpha^{r^2},\quad \ldots,\quad \alpha^{r^{p-2}}, \tag{3}$$

où r est une racine primitive de la congruence

$$x^{p-1}-1\equiv 0 \pmod p, \tag{4}$$

c'est-à-dire un nombre tel que r^k-1 ne peut être divisible par p pour $k<p-1$. Il est facile de voir que tous les termes de la suite (2) sont différents.

Soit β une racine arbitraire (1 excepté) de

$$x^{p-1}-1=0.$$

Nous aurons à considérer dans la suite le produit de

$$\left\{\begin{array}{l} V_1=\alpha+\beta\alpha^{r}+\beta^2\alpha^{r^2}+\ldots+\beta^{p-2}\alpha^{r^{p-2}} \\ \text{par} \\ V_2=\alpha+\beta^{-1}\alpha^{r}+\beta^{-2}\alpha^{r^2}+\ldots+\beta^{-(p-2)}\alpha^{r^{p-2}}; \end{array}\right. \tag{16}$$

les termes en β^n sont

$$\beta^n\left(\alpha^{r^n+1}+\alpha^{r(r^n+1)}+\alpha^{r^2(r^n+1)}+\ldots+\alpha^{r^{p-2}(r^n+1)}\right).$$

Si l'on pose $\alpha_1+\alpha^{r^n-1}$, α_1 sera racine de (1) et l'on aur

pour expression de la quantité entre parenthèses

$$\alpha_1 + \alpha_1^r + \alpha_1^{r^2} + \ldots + \alpha_1^{r^{p-2}}.$$

Si α_1 n'est pas égal à 1, ceci représente la somme des racines de l'équation (2), c'est-à-dire -1. Si, au contraire, $\alpha_1 = 1$, cette somme est égale à $p-1$; c'est ce qui a lieu si

$$r^n + 1 \equiv 0 \pmod p,$$

d'où l'on tire

$$n = \frac{p-1}{2};$$

le produit cherché sera alors

$$-\left(1 + \beta + \beta^2 + \ldots + \beta^{p-2} - \beta^{\frac{p-1}{2}}\right) + (p-1)\beta^{\frac{p-1}{2}},$$

et comme

$$1 + \beta + \beta^2 + \ldots + \beta^{p-2} = 0,$$

on aura

$$(7) \qquad V_1 V_2 = p\beta^{\frac{p-1}{2}} = \pm p,$$

car $\beta^{\frac{p-1}{2}}$ est égal à 1 ou à -1.

Dans le premier cas, on peut réunir dans les deux facteurs V_1 et V_2 les termes éloignés l'un de l'autre de $\frac{p-1}{2}$ rangs; deux semblables termes sont

$$\beta^n \alpha^{r^n} \quad \text{et} \quad \beta^{n+\frac{p-1}{2}} \alpha^{r^{n+\frac{p-1}{2}}} = \beta^n \alpha^{-r^n};$$

p divisant $r^{\frac{p-1}{2}} + 1$, p divise

$$\left(r^{\frac{p-1}{2}} - 1\right)\left(r^{\frac{p-1}{2}} + 1\right)$$

et ne divise pas le premier facteur; la somme de nos deux

termes est alors

$$S = \beta^n(\alpha^{r^n} + \alpha^{-r^n}),$$

ou si, par exemple,

$$\alpha = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p},$$

et si l'on pose

$$\frac{2\pi}{p} = a,$$

on a

$$S = 2\beta^n \cos r^n a.$$

Si l'on désigne alors par γ une racine de

(8) $$x^{\frac{p-1}{2}} - 1 = 0,$$

et si l'on fait $p = 2\mu + 1$, on aura

(9) $$4V_1V_2 = p,$$

où

$$V_1 = \cos a + \gamma\cos ra \quad + \ldots + \gamma^{\mu-1}\cos r^{\mu-1}a,$$
$$V_2 = \cos a + \gamma^{-1}\cos ra + \ldots + \gamma^{-(\mu-1)}\cos r^{\mu-1}a.$$

86. Si l'on pose

$$x^r = \theta(x),$$

les racines de l'équation donnée (2) pourront se mettre sous la forme

$$x,\quad \theta(x),\quad \theta^2(x),\quad \ldots,\quad \theta^{p-2}(x),$$

où $\theta^{p-1}(x) = x$; cette équation appartient donc à la classe des équations étudiées (79), et les racines sont des sommes de termes de la forme

$$\sqrt[p-1]{\upsilon},$$

υ désignant une fonction rationnelle des coefficients et de β. α peut donc s'exprimer au moyen de radicaux, si la même chose a lieu pour β; comme le calcul de β dépend à son tour de la résolution d'équations binomes dont les degrés sont des nombres premiers inférieurs à p, on finit, par des réductions successives, par tomber sur des équations que l'on peut ré-

soudre et, par suite, la proposée est résoluble au moyen de radicaux.

Les termes de α sont conjugués deux à deux ; par exemple

$$\sqrt[p-1]{\upsilon_1} \quad \text{et} \quad \sqrt[p-1]{\upsilon_{n-1}}$$

sont conjugués, etc. Ces deux radicaux sont V_1 et V_2 dont le produit est $\pm p$. Leur module est $\sqrt{p}$. Les arguments s'obtiennent en divisant, par les facteurs premiers de $p-1$, un angle que l'on peut construire. Si le nombre premier p est de la forme

$$p = 2^k + 1, \tag{10}$$

$p-1$ ne contiendra pas d'autres facteurs premiers que 2, *on pourra donc, dans ce cas, partager la circonférence en p parties égales, au moyen de cercles et de lignes droites, car on n'aura à construire que des expressions rationnelles, à partager des angles en deux parties égales et à construire la racine carrée de p.*

87. Au lieu de traiter comme nous l'avons fait l'équation donnée, on peut la traiter comme une équation réciproque et la réduire à une autre de degré μ, celle-ci conserve le caractère d'équation abélienne. En effet, ses racines étant des sommes de racines conjuguées de l'équation binome sont de la forme

$$2\cos a, \quad 2\cos ra, \quad 2\cos r^2 a, \quad \ldots, \quad 2\cos r^{\mu-1} a, \tag{11}$$

et l'on sait que $\cos ra$ est fonction rationnelle de $\cos a$. Si l'on fait pour cette équation le produit

$$\sqrt[\mu]{\upsilon_1}\,\sqrt[\mu]{\upsilon_{n-1}},$$

on retrouve le produit (9) dont la valeur est p.

C'est Gauss qui a résolu, pour la première fois, l'équation binome; il a fait voir que la circonférence pouvait être partagée en $p = 2^k + 1$ parties égales quand p était premier, et

cela en partageant des angles en deux parties égales et en construisant $\sqrt{p}$.

Plus tard, Abel a généralisé la méthode de Gauss.

Division de la circonférence en 17 parties égales.

88. La division de la circonférence en dix-sept parties égales dépend de l'équation

$$x^{17} - 1 = 0; \tag{1}$$

si on la divise par $x - 1$ et si l'on réduit l'équation réciproque ainsi obtenue, on obtient la transformée

$$x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 - 10x^3 - 10x^2 - 4x + 1 = 0. \tag{2}$$

Les racines de cette équation sont

$$x = 2\cos\frac{2k\pi}{17},$$

où $k = 1, 2, \ldots, 8$.

L'équation (2) étant du degré 2^3 pourra être résolue par la méthode développée (80), à l'aide de trois équations du second degré; mais nous préférons faire usage de l'équation primitive du 16e degré.

La plus petite racine primitive de $x^{16} \equiv 1 \pmod{17}$ est 3; on prendra alors $r = 3$, et les racines seront

$$\begin{array}{cccccccc} \alpha, & \alpha^3, & \alpha^9, & \alpha^{10}, & \alpha^{13}, & \alpha^5, & \alpha^{15}, & \alpha^{11} \\ \alpha^{-1}, & \alpha^{-3}, & \alpha^{-9}, & \alpha^{-10}, & \alpha^{-13}, & \alpha^{-5}, & \alpha^{-15}, & \alpha^{-11}. \end{array}$$

Posons

$$\left\{ \begin{aligned} y_1 &= \alpha + \alpha^9 + \alpha^{13} + \alpha^{15} + \alpha^{-1} + \alpha^{-9} + \alpha^{-13} + \alpha^{-15}, \\ y_2 &= \alpha^3 + \alpha^{10} + \alpha^5 + \alpha^{11} + \alpha^{-3} + \alpha^{-10} + \alpha^{-5} + \alpha^{-11}, \end{aligned} \right. \tag{4}$$

alors on a

$$y_1 + y_2 = -1.$$

Le produit $y_1 y_2$ est rationnel, car si l'on échange α avec une autre racine il ne change pas de valeur; car si l'on échange α

avec une racine du même groupe y_1 et y_2 ne changent pas; si l'on échange α avec une racine d'un autre groupe y_1 et y_2 s'échangent entre eux. Comme le produit de deux racines est encore une racine, $y_1 y_2$ est la somme de 64 racines parmi lesquelles ne se trouve pas l'unité, deux racines conjuguées se trouvant dans le même groupe; comme le produit est symétrique chaque racine y entre quatre fois.

Enfin, comme la somme des racines est -1, on a

$$y_1 y_2 = -4,$$

et y_1 et y_2 sont racines de

$$(5) \qquad y^2 + y - 4 = 0.$$

Maintenant posons

$$(6) \quad \begin{cases} \alpha + \alpha^{13} + \alpha^{-1} + \alpha^{-13} = z_1; & \alpha^3 + \alpha^5 + \alpha^{-3} + \alpha^{-5} = z_3, \\ \alpha^9 + \alpha^{15} + \alpha^{-9} + \alpha^{-15} = z_2; & \alpha^{10} + \alpha^{11} + \alpha^{-10} + \alpha^{-11} = z_4, \end{cases}$$

on aura

$$(7) \qquad z_1 + z_2 = y_1; \qquad z_3 + z_4 = y_2.$$

L'équation qui a pour racines les 8 termes de y_1 est du huitième degré; l'un de ses coefficients est $-y_1$ et les autres sont fonctions rationnelles de celui-ci. $z_1 z_2$ doit donc pouvoir s'exprimer rationnellement en y_1, car il n'est pas altéré quand on échange les racines contenues dans y_1; le produit en question a 16 termes qui sont tous racines; parmi ceux-ci se trouve α^{10} qui appartient à y_2 et α^8 qui appartient à y_1; les autres termes de y_1 et y_2 doivent donc se trouver aussi parmi les 16 termes en question; on a donc

$$z_1 z_2 = y_1 + y_2 = -1,$$

et, en remplaçant α par α^3,

$$z_3 z_4 = -1;$$

les z sont donc racines de

$$(8) \qquad z^2 - y_1 z - 1 = 0 \qquad \text{et} \qquad z^2 - y_2 z - 1 = 0.$$

Si l'on pose enfin

$$\alpha + \alpha^{-1} = t_1,$$

$$\alpha^{13} + \alpha^{-13} = t_2,$$

$$t_1 + t_2 = z_1; \qquad t_1 t_2 = z_3,$$

comme $t_1 t_2$ est rationnel en y_1 et z_1, il doit en être de même de z_3, et l'on a, en effet,

$$z_1^2 = z_2 + 2z_3 + 4 \qquad \text{ou} \qquad 2z_3 = z_1^2 + z_1 - y_1 - 4;$$

t_1 et t_2 sont donc racines de

$$(9) \qquad t^2 - z_1 t + z_3 = 0.$$

On peut donner six expressions analogues à celles qui sont données pour t_1 et t_2. Ces huit valeurs sont racines de l'équation réciproque du huitième degré à laquelle se ramène la proposée; ces valeurs sont

$$2\cos a; \qquad 2\cos 2a; \qquad \ldots; \qquad 2\cos 8a,$$

où

$$a = \frac{2\pi}{17}.$$

Le côté du polygone de 34 côtés inscrit dans le cercle de rayon 1 a pour expression

$$2\sin\frac{\pi}{34} = 2\cos\frac{8\pi}{17} = 2\cos 4a$$

et se trouve parmi ces racines; on les construit facilement au moyen de cercles et de droites, à l'aide de trois équations du second degré, en construisant d'abord y et z. Ainsi, on construit le polygone de 17 côtés et, en joignant les sommets de deux en deux, celui de 34 côtés.

Réduction de l'équation $x^{13} = 1$.

89. Nous appliquerons encore notre méthode au cas où $p = 13$; ici $r = 2$, et, en faisant abstraction de la racine 1, les autres sont

$$\alpha, \quad \alpha^2, \quad \alpha^4, \quad \alpha^8, \quad \alpha^3, \quad \alpha^6, \quad \alpha^{-1}, \quad \alpha^{-2}, \quad \alpha^{-4}, \quad \alpha^{-8}, \quad \alpha^{-3}, \quad \alpha^{-6}.$$

Si l'on pose

$$y_1 = \alpha + \alpha^4 + \alpha^3 + \alpha^{-1} + \alpha^{-4} + \alpha^{-3},$$
$$y_2 = \alpha^2 + \alpha^8 + \alpha^6 + \alpha^{-2} + \alpha^{-8} + \alpha^{-6},$$

on a

$$y_1 + y_2 = -1; \qquad y_1 y_2 = -3,$$

et l'on a, pour calculer y_1 et y_2,

$$y^2 + y - 3 = 0.$$

Posons

$$z_1 = \alpha + \alpha^{-1}; \qquad z_2 = \alpha^4 + \alpha^{-4}; \qquad z_3 = \alpha^3 + \alpha^{-3},$$

et, par suite,

$$z_1 + z_2 + z_3 = y_1,$$
$$z_1 z_2 + z_1 z_3 + z_2 z_3 = -1,$$
$$z_1 z_2 z_3 = 2 + y_2 = 1 - y_1;$$

les six valeurs de $2\cos\frac{2k\pi}{13}$ seront déterminées par les équations

$$y^2 + y - 3 = 0,$$
$$z^3 - yz^2 - z + y - 1 = 0.$$

Propriété de l'équation $\frac{x^p - 1}{x - 1} = 0$ où p est premier.

90. L'équation

$$(1) \qquad X = \frac{x^p - 1}{x - 1} = 0,$$

où p est un nombre premier, a pour racines

$$\alpha, \quad \alpha^r, \quad \alpha^{r^2}, \quad \ldots, \quad \alpha^{r^{p-2}};$$

si l'on pose, comme plus haut,

$$(2) \qquad \begin{cases} y_1 = \alpha + \alpha^{r^2} + \alpha^{r^4} + \ldots + \alpha^{r^{p-3}}, \\ y_2 = \alpha^r + \alpha^{r^3} + \alpha^{r^5} + \ldots + \alpha^{r^{p-2}}, \end{cases}$$

on a

$$y_1 + y_2 = -1;$$

p peut être de la forme $4n + 1$ ou $4n + 3$.

1° $p = 4n + 1$. — Les racines conjuguées se trouvent dans le même groupe; en sorte que $y_1 y_2$ ne contient pas le terme 1. Le nombre des termes de $y_1 y_2$ est $4n^2$ et chaque racine doit y entrer n fois; on a donc

$$y^2 + y - n = 0$$

et

$$y = \frac{-1 \pm \sqrt{p}}{2}. \tag{3}$$

L'équation dont les racines sont les termes de y_1 a ses coefficients de la forme $a + by_1$, a et b désignant des nombres entiers; si l'on forme la somme des produits de q racines pour calculer les coefficients de l'équation, on obtient une somme dont chaque terme est une racine; ces racines sont les unes égales à 1, les autres sont des termes de y_1 ou de y_2; mais, si un terme de y_1 se trouve dans le produit, ils doivent s'y trouver tous. La somme a donc la forme $ay_1 + by_2 + c$ ou $(a - b)y_1 + c - b$, où a, b, c sont entiers et où l'on a

$$2n(a + b) + c = C_q(2n),$$

ces deux nombres étant tous deux l'expression du nombre des termes qui entrent dans le coefficient calculé.

Si l'on échange α en α^r, et, par suite, y_1 en y_2, on obtient l'équation dont les racines sont les termes de y_2, les deux équations se distinguent seulement l'une de l'autre par le signe de $\sqrt{p}$. Il n'y entre pas d'autres dénominateurs que 2; alors on peut écrire ces équations ainsi

$$\frac{Y + \sqrt{p}Z}{2} = 0 \quad \text{et} \quad \frac{Y - \sqrt{p}Z}{2} = 0,$$

où Y et Z ont des coefficients entiers, et on a identiquement

$$4X = Y^2 - pZ^2.$$

Y est de degré $\frac{p-1}{2}$, Z de degré $\frac{p-3}{2}$; comme les deux équations que nous venons de former sont réciproques, on voit

que dans Y et Z les coefficients formeront des suites symétriques, comme dans les équations réciproques.

2° $p = 4n + 3$. — Les racines qui entrent dans y_1 sont les inverses de celles qui entrent dans y_2 ; parmi les $(2n+1)^2$ termes de $y_1 y_2$ se trouve l'unité $2n+1$ fois; chaque autre racine entre n fois; on a alors

$$y^2 + y + n + 1 = 0,$$

$$y = \frac{-1 \pm \sqrt{-p}}{2},$$

et, en procédant comme plus haut, on a

$$4X = Y^2 + pZ^2;$$

les deux équations ne diffèrent, comme dans le cas précédent, que par le signe de $\sqrt{-p}$, mais elles ne sont plus réciproques; l'une se déduit de l'autre en changeant x en $\frac{1}{x}$ et en chassant les dénominateurs; les coefficients de Z ont les mêmes propriétés que plus haut, et les coefficients de Y sont égaux et de signes contraires deux à deux.

Notre développement n'est pas applicable au cas où $p = 3$; dans ce cas

$$4(x^2 + x + 1) = Y^2 + 3Z^2;$$

$$Y = 2x + 1; \qquad Z = 1,$$

ou

$$Y = x + 2; \qquad Z = x,$$

ou

$$Y = x - 1; \qquad Z = x + 1.$$

Les théorèmes que nous venons de démontrer sur les polynomes X trouvent leur application dans la théorie des nombres (Dirichlet, *Journal de Crelle,* t. 17).

CHAPITRE VII.

ÉQUATIONS RÉSOLUBLES A L'AIDE DE RACINES CARRÉES.

Forme des racines.

91. Soit x_1 une racine d'une équation irréductible donnée que nous supposerons résoluble au moyen d'expressions rationnelles et de racines carrées; lorsque nous dirons qu'une expression contient n racines carrées, il faudra sous-entendre que ces racines sont distinctes; nous dirons qu'une expression qui ne contient que des racines carrées d'expressions rationnelles est une expression du premier ordre; une expression qui contiendra des racines carrées d'expressions du premier ordre seulement sera du second ordre et ainsi de suite.

Si les radicaux qui entrent dans x_1 sont liés entre eux par une équation du premier degré à coefficients rationnels, on en profitera pour réduire le nombre des radicaux contenus dans x_1. Lorsque x_1 sera ainsi ramené à contenir le plus petit nombre possible de radicaux, on fera évanouir les radicaux qui entreront en dénominateurs; on n'introduira pas, par cette opération, de nouveaux radicaux, cette opération se faisant par de simples multiplications qui peuvent se faire de façon qu'on n'introduise pas de nouveaux radicaux. Alors les radicaux n'entrent dans x_1 qu'avec l'exposant 1; car une puissance paire d'un radical est une expression radicale d'un ordre moins élevé; il en résulte aussi que *toute fonction rationnelle d'un radical entrant dans x_1 peut s'exprimer en fonction rationnelle du premier degré par rapport à ce radical.*

Si l'on change les signes des radicaux qui entrent dans

l'expression de x_1 de toutes les manières possibles, x_1 prendra de nouvelles valeurs $x_2, x_3, \ldots, x_\mu$ et, si x_1 contient p radicaux, x_1 prendra 2^p valeurs; mais ces 2^p valeurs ne sont pas toujours distinctes; c'est ainsi que

$$\sqrt{a+\sqrt{b}}+\sqrt{a-\sqrt{b}}$$

ne change pas quand on change le signe de $\sqrt{b}$.

Si x_1 est racine d'une équation irréductible

$$(1) \qquad f(x) = 0$$

$x_2, x_3, \ldots, x_\mu$ sont racines de la même équation.

En effet, remplaçons x par x_1 dans $f(x)$: comme il n'existe pas de relations entre les radicaux qui entrent dans x_1, les coefficients des radicaux qui entreront dans l'équation ainsi obtenue devront être nuls. Les équations qui en résultent et qui expriment que x_1 est racine, à leur tour contiendront des radicaux dont les coefficients devront être nuls et ainsi de suite; on arrive de la sorte à des équations qui ne contiennent plus que des quantités rationnelles, qui ne dépendront pas des signes des radicaux qui entraient dans x_1 et qui seront satisfaits, quels que soient ces signes. Si donc l'équation (1) admet pour racine x_1, elle admettra aussi pour racines $x_2, x_3, \ldots, x_\mu$.

Maintenant on peut poser

$$x_1 = A + B\sqrt{c},$$

où $\sqrt{c}$ est un radical qui n'entre pas sous un autre signe radical; $\sqrt{c}$ n'entre pas alors dans l'expression de A ou de B, qui peuvent contenir d'autres radicaux; posons alors

$$x_2 = A - B\sqrt{c};$$

le produit

$$(x - x_1)(x - x_2)$$

ne contiendra pas $\sqrt{c}$ si l'on forme des produits analogues pour toutes les autres racines en changeant les signes des radicaux se trouvant en A et B; on obtient l'expression

$$(x - x_1)(x - x_2), \ldots, (x - x_\mu)$$

transformée en un produit de 2^{p-1} facteurs du second degré, qui se déduisent de l'un d'eux, en changeant les signes des radicaux de toutes les manières possibles. Deux de ces facteurs sont de la forme

$$x^2 + (A_1 + B_1\sqrt{c})\,x + A_2 + B_2\sqrt{c_1},$$
$$x^2 + (A_1 - B_1\sqrt{c})\,x + A_2 - B_2\sqrt{c_1},$$

et leur produit du quatrième degré dont le premier terme est x^4 ne contient pas $\sqrt{c_1}$. Si l'on traite ces facteurs du quatrième degré d'une façon analogue et si l'on continue ainsi de suite, on finit par trouver une équation du degré 2^p à coefficients rationnels admettant les racines $x_1, x_2, \ldots, x_\mu$. Si elle est irréductible, elle doit se confondre avec l'équation donnée; mais il peut arriver que plusieurs valeurs de x soient égales, en sorte que l'équation obtenue soit réductible. Dans ce cas elle admettra un même nombre de fois toutes les racines de $f(x) = 0$; sans quoi, en divisant par une puissance convenable de $f(x)$, on pourrait obtenir une équation admettant une partie seulement des racines de $f(x) = 0$; le degré de l'équation donnée doit donc être un diviseur de 2^p. Donc

Une équation irréductible qui peut être résolue au moyen d'extractions de racines carrées doit être d'un degré égal à une puissance de 2 et ses racines ne diffèrent les unes des autres que par les signes des radicaux.

92. *Une racine d'une équation irréductible de degré 2^p qui peut être résolue à l'aide de racines carrées peut s'exprimer au moyen de p radicaux.*

Si dans l'équation

$$f(x) = 0 \tag{1}$$

on remplace x par $\frac{k}{x}$, si l'on chasse les dénominateurs et si l'on cherche par les méthodes connues le plus grand commun diviseur des premiers membres des deux équations, on

obtient un reste du premier degré

$$Mx + N$$

et le dernier diviseur peut être représenté par

$$Ax^2 + Bx + C,$$

M, N, A, B, C désignant des fonctions entières de k et des quantités connues. Soient x_1 et x_2 deux racines de l'équation (1) : si l'on fait $k = x_1 x_2$, x_1 et x_2 seront des racines communes aux deux équations et l'on aura

$$x_1 + x_2 = -\frac{B}{A}; \qquad x_1 x_2 = \frac{C}{A} = k.$$

La forme la plus générale d'un facteur du second degré de $f(x)$ en fonction du produit de deux racines est donc

$$x^2 + \varphi(k)x + k,$$

φ désignant une fonction rationnelle.

Quand k sera connu, les deux racines seront ainsi données par une équation du second degré, c'est-à-dire que leur expression contiendra un radical de plus que celle de k.

k, étant un produit de deux racines, sera déterminé par une équation de degré

$$\frac{2^p(2^p - 1)}{2} = 2^{p-1}(2^p - 1).$$

Comme k peut s'exprimer au moyen de racines carrées, l'équation en k devra pouvoir se décomposer en d'autres dont les degrés seront des puissances de 2. Ces équations ne peuvent être toutes de degré 2^p ou de degré plus élevé, car une somme de pareilles puissances serait divisible par 2^p, ce qui n'a pas lieu avec le degré de l'équation déterminant k : le degré de l'une de ces équations doit donc être au plus égal à 2^{p-1}.

L'équation de degré 2^p pourra donc se résoudre au moyen de p racines carrées si celle du degré 2^{p-1} peut se résoudre au moyen de $n - 1$ racines carrées. Mais l'équation du second degré peut se résoudre au moyen d'une racine carrée ; le théo-

rème se trouve donc démontré. Cependant, il existe un cas qui demande à être examiné de plus près, à savoir celui dans lequel $f(x)$ et $f\left(\frac{k}{x}\right)$ ont un facteur commun de degré supérieur à deux. Cela ne peut arriver que si l'on a, pour des valeurs de p et q différentes de 1 et 2,

$$x_p = \frac{k}{x_q};$$

on aura alors

$$x_1 x_2 = x_p x_q$$

et si l'on remplace x par $x + h$,

$$x_p x_q + h(x_p + x_q) + h^2 = x_1 x_2 + h(x_1 + x_2) + h^2;$$

cette formule ne peut avoir lieu quel que soit h; sans quoi l'équation donnée aurait des racines égales, ce qui est impossible, puisqu'elle est irréductible.

Si donc la démonstration tombait en défaut, on pourrait toujours transformer l'équation de manière que le cas en question ne se présente pas. Comme la transformation n'altère pas le nombre des radicaux qui entrent dans les expressions des racines, le théorème est vrai dans tous les cas.

93. Si, comme plus haut, on associe les facteurs

$$x - x_1, \quad x - x_2, \quad \ldots, \quad x - x_\mu$$

deux par deux, les nouveaux facteurs du second degré deux par deux et ainsi de suite, on se débarrasse chaque fois d'un radical; quand il ne reste plus qu'un radical $\sqrt{\alpha}$, on obtient deux facteurs qui ne diffèrent l'un de l'autre que par le signe de $\sqrt{\alpha}$; l'équation de degré 2^p peut alors se ramener à une autre de degré 2^{p-1} dans laquelle les coefficients contiennent $\sqrt{\alpha}$ et qui prendra la forme

$$\begin{aligned} x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots \\ + a_m \pm \sqrt{\alpha}\,(b_1 x^{m-1} + b_2 x^{m-2} + \ldots + b_m) = 0 \end{aligned}$$

où $m = 2^{p-1}$, et l'on peut toujours faire en sorte que le coef-

ficient de la plus haute puissance de x soit l'unité, sans que $\sqrt{\alpha}$ entre en dénominateur. Si l'équation donnée est

$$f(x) = 0,$$

il faut donc que l'on ait

$$f(x) = (x^m + a_1 x^{m-1} + \ldots + a_m)^2 \\ - \alpha(b_1 x^{m-1} + b_2 x^{m-2} + \ldots + b_m)^2.$$

$\sqrt{\alpha}$ est le dernier radical que l'on fait disparaître dans x_1, c'est-à-dire le premier qu'il faut calculer quand on veut évaluer x_1; si l'on a le choix entre plusieurs radicaux à calculer tout d'abord, $f(x)$ peut être ramenée de plusieurs manières à la forme que nous venons de considérer. Par exemple, si

$$x_1 = \sqrt{a} + \sqrt{b} + \sqrt{\sqrt{a} + \sqrt{b} + k},$$

on pourra ramener $f(x)$ aux deux formes

$$A^2 - aB^2 \quad \text{ou} \quad A^2 - bB^2,$$

où A est du quatrième degré et B du troisième.

Résolution de l'équation.

94. Pour abaisser l'équation donnée, on peut former l'équation qui a pour racines les valeurs de

$$(x_1 + x_2 + \ldots + x_m)(x_{m+1} + x_{m+2} + \ldots + x_{2m}).$$

Le degré g de cette équation est égal à la moitié du nombre de manières dont on peut prendre 2^{p-1} lettres sur 2^p ou

$$g = \frac{2^p!}{2(2^{p-1}!)^2}.$$

On peut montrer que ce nombre est impair; si l'on divise par 2 tous les facteurs pairs de $2^p!$ on obtient tous les facteurs de $2^{p-1}!$. Si donc u, u_1, u_2 désignent des nombres impairs, on aura

$$2^p! = 2^{2^{p-1}} . 2^{p-1}! \, u.$$

Si l'on remplace successivement p par $p-1$, $p-2$, ..., 1 et si l'on multiplie les équations ainsi obtenues, il vient

$$2^p! = 2^{2^p-1} u u_1 u_2 \ldots;$$

le dénominateur de g étant $2^{2^p-1} u_1^2 u_2^2 \ldots$, ainsi

$$g = \frac{u}{u_1 u_2 \ldots},$$

ce qui est un nombre impair.

L'équation déduite de la proposée et que nous venons de considérer est résoluble par radicaux, si la proposée l'est, et elle doit se décomposer en équations dont les degrés sont des puissances de 2; or son degré est impair: donc l'une des équations dans lesquelles elle se décompose doit être du premier degré, de sorte que, parmi les valeurs que peut acquérir le produit que nous avons considéré, l'une est rationnelle; on peut la trouver dès que l'on a formé l'équation auxiliaire, car elle entre en facteur dans le dernier terme du premier membre de l'équation auxiliaire; comme on connaît en outre la somme des facteurs de ce produit, ceux-ci pourront se déterminer au moyen d'une équation du second degré à coefficients rationnels. On connaît donc la somme de m racines en fonction d'un radical carré et les autres fonctions symétriques de ces m racines peuvent s'exprimer rationnellement à l'aide de la somme trouvée et des quantités connues; l'équation qui détermine ces m racines a donc la forme

$$x^m + (a_1 + b_1\sqrt{\alpha})x^{m-1} + (a_2 + b_2\sqrt{\alpha})x^{m-2} + \ldots + a_m + b_m\sqrt{\alpha} = 0,$$

où a_1, b_1, a_2, ..., a_m, b_m et α sont rationnels. Si l'on change $+\sqrt{\alpha}$ en $-\sqrt{\alpha}$, on obtient l'équation qui donne les m autres racines.

Si l'on traite de même l'équation réduite, en regardant $\sqrt{\alpha}$ comme une quantité connue, on obtient une équation de degré 2^{p-2} dont les coefficients sont fonctions de $\sqrt{\alpha}$ et d'un nouveau radical carré. Ici se présente une difficulté : la racine que l'on cherche et qui doit être considérée comme ration-

nelle est en réalité de la forme $b+c\sqrt{\alpha}$ et doit être facteur d'une expression de la même forme, à savoir le dernier terme de l'équation; mais on peut tourner la difficulté en changeant x en $y+z\sqrt{\alpha}$ et en décomposant l'équation en deux autres ayant pour racines b et c.

Condition pour qu'il soit possible de résoudre l'équation.

95. En suivant la marche que nous venons d'indiquer, il est toujours possible de résoudre une équation résoluble à l'aide de radicaux carrés. Mais en pratique il devient déjà très pénible de résoudre l'équation du huitième degré. On peut souvent simplifier les calculs en faisant usage du théorème suivant :

S'il est possible de réduire de moitié le degré de l'équation $f(x)=0$, en extrayant la racine carrée de $f(x)$, on doit trouver un reste qui, multiplié par une puissance de 2, est divisible par α, $\sqrt{\alpha}$ désignant la racine carrée à laquelle on est conduit en effectuant la réduction.

Supposons que l'équation soit

$$(1) \qquad x^{2m}+A_1x^{2m-1}+\ldots+A_m=0$$

et puisse être ramenée à la forme

$$(2) \quad (x^m+a_1x^{m-1}+\ldots+a_m)^2-\alpha(b_1x^{m-1}+b_2x^{m-2}+\ldots+b_m)^2=0;$$

supposons que l'extraction de la racine carrée donne pour (1)

$$(3) \qquad (x^m+k_1x^{m-1}+k_2x^{m-2}+\ldots+k_m)^2+R_{m-1}=0,$$

R_{m-1} étant, au plus, de degré $m-1$; alors on a identiquement

$$(4) \begin{cases} [2x^m+(a_1+k_1)x^{m-1}+(a_2+k_2)x^{m-2}+\ldots+a_m+k_m] \\ \quad\times[(a_1-k_1)x^{m-1}+(a_2-k_2)x^{m-2}+\ldots+a_m-k_m] \\ \quad=\alpha(b_1x^{m-1}+b_2x^{m-2}+\ldots+b_m)^2+R_{m-1} \end{cases}$$

et, en égalant les coefficients de x^{2m-1}, x^{2m-2}, ..., x^m où

le reste est sans influence,

$$(5)\quad \left\{\begin{array}{l} 2(a_1-k_1)=0, \\ 2(a_2-k_2)+(a_1+k_1)(a_1-k_1)=\alpha b_1^2, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ 2(a_p-k_p)+(a_1+k_1)(a_{p-1}-k_{p-1})+\ldots=\alpha A, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ 2(a_m-k_m)+(a_1+k_1)(a_{m-1}-k_{m-1})+\ldots \\ \qquad\qquad +(a_{m-1}+k_{m-1})(a_1-k_1)=\alpha B. \end{array}\right.$$

αA et αB désignant des quantités divisibles par α.

La première de ces équations montre que $a_1=k_1$; la seconde que a_2-k_2, abstraction faite du facteur 2, est divisible par α; la troisième que a_3-k_3 est divisible par α, et ainsi de suite; la dernière montre que a_m-k_m est encore divisible par α; α est donc facteur du premier membre de l'identité (4) et par suite de R_{m-1}.

Si la racine contient plusieurs radicaux du premier ordre, chacun de ceux-ci peut être soumis à la même discussion que $\sqrt{\alpha}$, et tous les facteurs des quantités rationnelles α doivent se trouver dans les termes de R_{m-1}.

Considérons, par exemple, l'équation à laquelle on ramène $x^{17}-1=0$, à savoir

$$f(x)=x^8+x^7-7x^6-6x^5+15x^4+10x^3-10x^2-4x+1=0;$$

l'extraction de la racine carrée donne

$$2^{12}R_{m-1}=-17{,}32x^3-17.88x^2-17.92x-17.1273;$$

l'équation peut en réalité s'écrire

$$x^4+\frac{1}{2}x^3-\frac{3}{2}x^2+2x-1=\pm\frac{\sqrt{17}}{2}(x^3+x^2-2x).$$

Application à un problème de Géométrie.

96. Les équations que l'on peut résoudre par de simples extractions de racines carrées ont une importance toute particulière en Géométrie, car tout problème de Géométrie

résoluble au moyen de la règle et du compas doit conduire à une semblable équation. Toute construction de ce genre se ramène à ces problèmes élémentaires : faire passer une droite par deux points; décrire, d'un point donné comme centre, une circonférence de rayon donné; en répétant ces constructions, la Géométrie analytique permet de calculer les éléments inconnus en fonction de ceux qui sont donnés ; comme ces calculs ne conduisent jamais à des équations d'un degré plus élevé que le second, *il faut que les éléments inconnus puissent se déduire des données par de simples extractions de racines carrées.*

Il résulte de là qu'il est impossible de partager un angle en trois parties égales au moyen de la règle et du compas. On peut, en effet, se proposer de construire le cosinus de cet angle et, comme ce cosinus est racine d'une équation irréductible du troisième degré, il ne peut pas s'exprimer au moyen de racines carrées.

La plupart des constructions reviennent à la détermination d'un point qui lui-même se trouve déterminé par l'intersection de deux lieux géométriques. Si l'un d'eux est une droite dans une position quelconque et si l'autre est une courbe indépendante, on peut déterminer l'ordre de cette courbe si la construction du point peut se faire à l'aide de la règle et du compas. D'une manière moins générale, on peut avoir à déterminer la courbe lorsque la droite renferme un paramètre variable, par exemple quand elle doit passer par un point fixe.

97. Supposons que l'on se donne un faisceau de droites dont le sommet soit à l'origine des coordonnées et proposons-nous de *trouver les courbes dont les intersections avec une droite quelconque du faisceau peuvent être déterminées à l'aide de la règle et du compas.*

Nous supposerons que la courbe ne passe pas par l'origine; prenons des coordonnées polaires et posons

$$(1) \qquad x = mr; \qquad y = nr;$$

l'équation de la courbe prend la forme

$$(2) \qquad a + br + cr^2 + \ldots = 0,$$

où a n'est pas nul et où $a, b, c, \ldots$ sont des fonctions homogènes des degrés 0, 1, 2, ... de m et de n.

Si le problème peut être résolu avec la règle et le compas, cette équation doit pouvoir se résoudre pour toute valeur de m et de n; il existe sans doute entre m et n une relation en sorte que leur rapport seul est arbitraire; mais on peut remplacer m et n par mk et nk, si l'on change en même temps r en $\frac{r}{k}$, et l'on peut, par cete raison, regarder m et n comme indépendants.

D'après nos hypothèses les constantes qui entrent dans l'équation de la courbe sont indépendantes de m et de n. Il est facile de voir que l'équation (2) est irréductible si la courbe est indécomposable.

Si l'équation (2) est susceptible de se résoudre au moyen de racines carrées, elle devra pouvoir se ramener à la forme

$$(3) \qquad k(A + Br + Cr^2, \ldots)^2 = k_1(A_1 + B_1 r + C_1 r^2, \ldots)^2,$$

où k et k_1 sont des fonctions entières homogènes de m et n; (3) n'est pas nécessairement identique à (2), car on peut avoir supprimé un facteur par la division. En comparant les équations, on voit que ce facteur est

$$\frac{kA^2 - k_1 A_1^2}{a} \qquad \text{ou} \qquad \varphi = kA^2 - k_1 A_1^2;$$

car a est indépendant de m et n et on peut le supprimer sans changer la forme de nos équations. On peut supposer que k et k_1 n'ont pas de facteur commun, car on pourrait le faire disparaître par la division; on peut supposer en outre que φ n'a pas de facteur commun avec k et k_1; car un facteur appartenant à φ et à k_1 appartiendrait à A, B, C, ... et pourrait être supprimé par division sans changer la forme de l'équation.

On peut mettre (3) sous la forme

$$\begin{aligned}&[A\sqrt{k} + A_1\sqrt{k_1} + (B\sqrt{k} + B_1\sqrt{k_1})r + \ldots]\\ &\quad\times [A\sqrt{k} - A_1\sqrt{k_1} + (B\sqrt{k} - B_1\sqrt{k_1})r + \ldots] = 0.\end{aligned}$$

Si l'on multiplie le premier facteur par $A\sqrt{k} - A_1\sqrt{k_1}$, le second par $A\sqrt{k} + A_1\sqrt{k_1}$, on obtient la forme

$$[\varphi + (M + N\sqrt{kk_1})r + (M_1 + N_1\sqrt{kk_1})r^2 + \ldots]$$
$$\times [\varphi + (M - N\sqrt{kk_1})r + (M_1 - N_1\sqrt{kk_1})r^2 + \ldots] = 0$$

et le premier membre doit être divisible par φ^2.

Nous allons montrer que chacun des facteurs est divisible par φ. Si l'on forme le produit des deux facteurs, chaque coefficient sera divisible par φ^2; or, en développant, on a

$$\varphi^2 + 2\varphi M r + \ldots$$

et l'on voit que φ doit être en facteur dans M. Si $m - \alpha n$ est en facteur dans φ, $m = \alpha n$ doit annuler un des deux facteurs, par exemple le premier; $m = \alpha n$ doit alors annuler $M + N\sqrt{kk_1}$ et, comme kk_1 n'a pas de facteur commun avec φ, il doit annuler N. Maintenant, considérons dans le produit le coefficient de r^2: en dehors des termes divisibles par φ^2, il n'entre que le terme $2M_1\varphi$ et nous voyons que M_1 doit être divisible par φ; nous en concluons, comme plus haut, que N_1 est divisible par φ; en continuant ainsi, on voit que tous les M et les N sont divisibles par φ. Si l'on divise les deux facteurs par φ, on obtient l'équation (3) dégagée du facteur φ et sans que sa forme soit modifiée; on peut donc supposer (2) et (3) identiques; alors on a $kA^2 - k_1A_1^2 = a$, a étant indépendant de m et n; a n'est pas nul et k et k_1 ne peuvent être tous deux constants (sans quoi l'équation serait réductible); les coefficients doivent être des fonctions homogènes de m et de n, parce que l'équation reste inaltérée par la substitution qui remplace m, n, r par mh, nh, $\frac{r}{h}$ et ne peut prendre la forme (3) que d'un nombre fini de manières; si donc k_1 contient m et n, A_1 doit être nul et k et A constants.

Si l'on pose $k_1 = 0$ dans (3), on détermine les valeurs de m et n pour lesquelles les points d'intersection d'une droite et de la courbe sont confondus deux à deux. *La courbe doit donc être une courbe d'ordre* 2^p *telle que du sommet du*

faisceau on puisse lui mener des sécantes dont les intersections coïncident deux à deux et, comme $A_1 = 0$, k_1 doit être au moins du second degré en m et n; le sommet du faisceau doit donc être le point d'intersection de deux droites jouissant de cette propriété et, s'il est arbitraire, le problème ne sera possible que si une droite coupe la courbe en deux points seulement. Donc :

En dehors des coniques, il n'existe pas de courbe dont les intersections avec une droite arbitraire puissent se déterminer à l'aide de la règle et du compas.

Et le principe de dualité montre que, *en dehors des coniques, il n'existe pas de courbe dont les tangentes menées par un point arbitraire puissent être construites avec la règle et le compas.*

Intersections d'un faisceau avec une courbe du quatrième ordre.

98. Nous allons considérer, en particulier, les courbes du quatrième ordre; leur équation doit être de la forme

$$(1) \qquad (A + Br + Cr^2)^2 = kr^2(Dr + E)^2.$$

Si E n'est pas nul, k est du deuxième degré; si E est nul, k doit être du quatrième degré. Dans le premier cas, on parvient à une équation de la forme

$$(2) \qquad S^2 = \lambda\, \alpha\beta\gamma^2,$$

où $S = 0$ représente une conique quelconque, où λ désigne une constante, $\gamma = 0$ une ligne droite, $\alpha = 0$, $\beta = 0$ deux droites du faisceau.

Dans le second cas, on a

$$S^2 = \lambda\, \alpha\beta\gamma\delta;$$

$\alpha = 0$, $\beta = 0$, $\gamma = 0$, $\delta = 0$ sont alors des droites arbitraires du faisceau.

La première équation appartient à une courbe du quatrième ordre avec deux points doubles déterminés par $S = 0$ et

$\gamma = 0$ et avec les tangentes doubles $\alpha = 0$, $\beta = 0$ qui se coupent au point donné et dont les points de contact se trouvent avec les points doubles sur la conique $S = 0$.

La deuxième équation est celle d'une courbe du quatrième ordre avec quatre tangentes doubles qui se coupent au point donné et dont les huit points de contact sont sur la conique $S = 0$.

Nous n'examinerons pas le cas où le point donné se trouve sur la courbe et y est un point multiple d'ordre q, l'ordre de la courbe cherchée s'élevant de q unités. Nous montrerons seulement comment on peut construire les intersections des courbes de la première classe avec les droites du faisceau au moyen de deux coniques.

L'équation (1) peut s'écrire

$$(C - D\sqrt{k})r^2 + (B - E\sqrt{k})r + A = 0.$$

Les racines étant r_1 et r_2, posons

$$\frac{2}{\rho_1} = \frac{1}{r_1} + \frac{1}{r_2}.$$

Si l'on change $\sqrt{k}$ en $-\sqrt{k}$ et ρ_1 en ρ_2, ρ_1 et ρ_2 seront déterminés par l'équation

$$(B^2 - kE^2)\rho^2 + 4AB\rho + 4A^2 = 0,$$

qui est celle d'une conique; cette conique, pour $E = 0$, se transforme en une droite double

$$B\rho + 2A = 0$$

qui est la polaire de l'origine par rapport à la conique $S = 0$.

Si E n'est pas nul, ρ_1 et ρ_2 sont confondus pour $k = 0$ et les tangentes doubles sont tangentes à la conique auxiliaire.

Comme les deux intersections fournies par la conique ne suffisent pas pour déterminer les quatre points d'intersection cherchés, nous ferons usage d'une seconde conique; on peut, par exemple, prendre celle dont les points d'intersection avec les droites du faisceau sont en division harmonique avec r_1 et

r_2, et également avec r_3 et r_4; ces points sont déterminés par les équations

$$2(x_1 x_2 + r_1 r_2) = (x_1 + x_2)(r_1 + r_2),$$
$$2(x_1 x_2 + r_3 r_4) = (x_1 + x_2)(r_3 + r_4).$$

On en déduit l'équation de la conique cherchée

$$(\mathrm{BD} - \mathrm{CE})x^2 + 2\,\mathrm{AD}x + \mathrm{AE} = 0.$$

Pour $\mathrm{E} = 0$, cette conique se décompose en deux droites, dont l'une passe par le point donné et dont l'autre est la droite trouvée plus haut. Dans ce cas, on ne peut pas opérer la réduction, tandis que, quand E est différent de zéro, on détermine facilement les quatre points d'intersection quand on a trouvé les intersections avec les coniques auxiliaires.

Inversement, on peut se donner deux coniques et se proposer de construire une courbe du quatrième ordre de l'espèce qu'on vient de considérer. Pour plus de détails, on peut consulter un Mémoire de l'auteur dans le *Tidsskrift* de Zeuthen pour 1874.

TROISIÈME PARTIE.

SUR LA RÉSOLUTION NUMÉRIQUE DES ÉQUATIONS.

CHAPITRE I.

SÉPARATION DES RACINES.

Limites des racines réelles.

99. La résolution algébrique des équations de degré supérieur au quatrième n'est, comme nous l'avons vu, possible que dans des cas particuliers. Lorsque l'on donne une équation à coefficients numériques, on peut cependant, sans connaître la forme algébrique des racines, déterminer leurs valeurs numériques avec telle approximation que l'on veut. Pour obtenir ces valeurs approchées, il faut d'abord séparer les racines, c'est-à-dire déterminer pour chaque racine deux nombres comprenant cette racine et pas d'autre racine ; s'il existe des racines égales, il faut connaître leur ordre de multiplicité. La séparation est facilitée quand on détermine d'abord les limites des racines, c'est-à-dire deux nombres comprenant toutes les racines réelles; on a plusieurs méthodes pour déterminer les limites des racines qui ne donnent cependant que des approximations très incertaines.

100. *Première méthode.* — Soit l'équation

$$x^n + a_1 x^{n-1} + \ldots - a_m x^{n-m} - \ldots - a_p x^{n-p} \ldots \pm a_n = 0,$$

où a_m est le premier coefficient négatif et a_p le plus grand coefficient négatif pris en valeur absolue. Pour $x > 1$, on a

$$x^n < a_p(x^{n-m} + x^{n-m+1} + \ldots + 1) = a_p \frac{x^{n-m+1} - 1}{x - 1},$$

donc aussi

$$x^n < a_p \frac{x^{n-m+1}}{x-1},$$

ou

$$x^{m-1}(x-1) < a_p,$$

ou

(1) $$x < 1 + \sqrt[m]{a_p}.$$

Cette valeur de x sera une limite supérieure des racines. On peut abaisser cette limite comme il suit. Posons

$$x = \frac{y}{\alpha},$$

et appliquons la formule trouvée pour la limite supérieure à l'équation en y, on a

$$y < 1 + \sqrt[m]{a_p \alpha^p},$$

on aura

(2) $$x < \frac{1}{\alpha} + \sqrt[m]{a_p \alpha^{p-m}}.$$

Comme α est un nombre positif arbitraire, on peut le choisir de manière à abaisser autant que possible la limite trouvée; cette valeur s'obtient en annulant la dérivée du second membre de (2), ce qui donne

$$\frac{1}{\alpha^2} = \frac{p-m}{m} \sqrt[m]{a_p}\, \alpha^{\frac{p}{m}-2},$$

où

$$\alpha^{\frac{p}{m}} = \frac{m}{p-m} a_p^{-\frac{1}{m}},$$

d'où

(3) $$x < \frac{p}{p-m}\left(\frac{p-m}{m}\right)^{\frac{m}{p}} \sqrt[p]{a_p} = p \sqrt[p]{\frac{a_p}{m^m(p-m)^{p-m}}},$$

formule que l'on ne peut employer si $m = p$; dans ce cas, (2) donne pour $\alpha = \infty$

(4) $$x < \sqrt[m]{a_m}.$$

On ne peut pas prendre ici pour a_p le plus grand coefficient

négatif de l'équation donnée, parce qu'il ne donne pas nécessairement le plus grand coefficient de l'équation en y; on doit, pour ce motif, prendre la limite la plus élevée, que l'on obtient quand on prend pour a_p tous les coefficients négatifs.

Exemple :

$$x^8 - x^7 + 5x^6 - 15x^5 - 47x^4 + x^3 - 711x^2 - 313x + 1 = 0;$$

les limites sont

$$1, \quad 3\sqrt[3]{\frac{15}{4}}, \quad 4\sqrt[4]{\frac{47}{27}}, \quad 6\sqrt[6]{\frac{711}{5^5}}, \quad 7\sqrt[7]{\frac{313}{6^6}},$$

d'où il résulte que 5 est une limite supérieure des racines positives. La plus basse limite en nombres entiers est en réalité 4.

Si l'on change x en $-x$ et si l'on cherche une limite supérieure des racines de l'équation transformée, on obtiendra une limite inférieure des racines négatives de l'équation proposée. On trouve ainsi

$$3\sqrt[6]{\frac{711}{16}} < 6,$$

en sorte que les racines réelles de l'équation considérée sont comprises entre -6 et $+5$.

Si l'on change x en $\frac{1}{x}$, on trouve, en appliquant les méthodes précédentes, que $\frac{1}{x}$ est compris entre deux limites $-k$ et k_1, alors x ne peut pas être compris entre $-\frac{1}{k}$ et $\frac{1}{k_1}$; la première de ces quantités est une limite supérieure des racines négatives, la seconde est une limite inférieure des racines positives.

101. *Deuxième méthode.* — On met l'équation sous la forme

$$f(x) = \varphi(x) - \varphi_1(x) + \varphi_2(x) = 0,$$

où $\varphi(x)$ désigne l'ensemble des termes précédant le pre-

mier terme négatif, $-\varphi_1(x)$ l'ensemble des termes négatifs, $\varphi_2(x)$ l'ensemble des termes positifs restants. Dans la différence

$$\varphi(x) - \varphi_1(x)$$

substituons des nombres positifs croissants jusqu'à ce que nous trouvions un nombre k qui rende cette différence positive; k sera une limite supérieure des racines positives. En effet, soit x^m la puissance la moins élevée de x dans $\varphi(x)$, la différence précédente peut s'écrire

$$x^m \left[\frac{\varphi(x)}{x^m} - \frac{\varphi_1(x)}{x^m} \right].$$

Or $\frac{\varphi(x)}{x^m}$ ne contenant que des coefficients et des exposants positifs sera croissant avec x, $\frac{\varphi_1(x)}{x^m}$ ne contenant que des exposants négatifs sera décroissant quand x croîtra. Une valeur de x supérieure à k rendra donc notre différence positive, et, par suite, $f(x)$ positif. Aucune valeur de x supérieure à k ne pouvant annuler $f(x)$, k sera une limite supérieure des racines.

Exemple. — Si, dans l'exemple ci-dessus, on change x en $-x$, on obtient l'équation

$$x^8 + x^7 + 5x^6 + 15x^5 - 47x^4 - x^3 - 711x^2 + 313x + 1 = 0.$$

Si, après avoir divisé par x^2, l'on cherche à rendre positif

$$x^6 + x^5 + 5x^4 + 15x^3 - (47x^2 + x + 711),$$

on voit que cela a lieu pour $x = 3$. Cette méthode fournit donc -3 comme limite supérieure des racines négatives, tandis que l'autre méthode donnait -6.

La méthode précédente peut être généralisée en décomposant $f(x)$ en plusieurs groupes de la forme $\varphi(x) - \varphi_1(x)$, où les coefficients de $\varphi(x)$ et de $\varphi_1(x)$ sont positifs, tous les termes de φ_1 étant de degrés inférieurs à ceux de $\varphi(x)$; une valeur de x qui rendra positives toutes ces différences sera évidemment une limite supérieure des racines positives.

102. *Méthode de Newton. — Si, dans les polynomes*

$$f(x),\quad f'(x),\quad f''(x),\quad \ldots,\quad f^n(x),$$

on substitue des valeurs croissantes de x jusqu'à ce que l'on trouve un nombre k qui les rende tous positifs, k sera une limite supérieure des racines.

En effet, on a

$$f(k+h) = f(k) + f'(k)\frac{h}{1} + f''(k)\frac{h^2}{1.2} + \ldots + h^n,$$

d'où il résulte que $f(k+h)$ sera positif si h est positif et si k a été déterminé comme il a été dit : $k+h$ ne peut donc être racine si h est positif, donc k est une limite supérieure des racines.

Cette méthode est plus pénible que les précédentes, mais elle donne, en général, des limites plus resserrées. Toutefois, les limites peuvent encore être trop élevées, car cette méthode fait, en outre, connaître des limites supérieures des racines de $f'(x)=0$, $f''(x)=0$, ..., et ces équations peuvent avoir des racines bien supérieures à celles de $f(x)=0$.

Un exemple servira à jeter quelque lumière sur la pratique de cette méthode.

Exemple :

$$x^5 + 5x^4 - 10x^3 + x^2 - 16x - 7 = 0,$$

		$x=0$	1	2	3
$f(x)$	$= x^5 + 5x^4 - 10x^3 + x^2 - 16x - 7.$			—	+
$f'(x)$	$= 5x^4 + 20x^3 - 30x^2 + 2x - 16\ldots$		—	+	
$\frac{f''(x)}{1.2}$	$= 10x^3 + 30x^2 - 30x + 1\ldots\ldots\ldots$		+		
$\frac{f'''(x)}{2.3}$	$= 10x^2 + 20x - 10\ldots\ldots\ldots\ldots\ldots$	—	+		
$\frac{f^{\text{IV}}(x)}{2.3.4}$	$= 5x + 5\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	+			
$f^{\text{V}}(x)$	$+\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$				

On commence par en bas, $x=0$ rend f^{V} positif, toute va-

leur supérieure rend f^{IV} positif, et l'on en a fini avec cette fonction, $x = 1$ rend positif $f'''(x)$ et $f''(x)$, mais $f'(x)$ négatif; pour $x = 2$, $f'(x)$ est positif, mais $f(x)$ est négatif et, comme finalement 3 rend $f(x)$ positif, c'est une limite supérieure des racines.

Nombre des racines comprises entre deux nombres donnés.

103. Soient α_1, α_2, α_3, ... les racines réelles de $f(x) = 0$, rangées par ordre de grandeurs croissantes; on a

$$f(x) = X(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)\ldots,$$

X déterminant les racines imaginaires et ne pouvant, par suite, s'annuler pour aucune valeur réelle de x. Si l'on prend x inférieur à α_1 et si on le fait croître jusqu'à ce qu'il passe par une valeur supérieure à la plus grande racine réelle, le signe d'un facteur et, par suite, le signe du produit changent chaque fois que x passe par une racine : $f(x)$ doit donc prendre le même signe pour des valeurs de x comprenant un nombre pair de racines et de signes opposés pour des valeurs de x comprenant un nombre impair de racines. Donc

Si $f(a)$ et $f(b)$ ont le même signe, il y a un nombre pair de racines entre a et b; si a et b sont de signes contraires, il y a un nombre impair de racines entre a et b.

Par exemple, si, dans une équation dont le dernier terme est $\pm a_n$, on fait successivement x égal à $-\infty$, 0 et $+\infty$, on obtient, pour $f(x)$

$$\pm\infty, \quad \pm a_n, \quad +\infty,$$

on a $+\infty$ pour $x = -\infty$ si l'équation est de degré pair et $-\infty$ si elle est de degré impair; il en résulte qu'*une équation de degré impair a au moins une racine réelle de signe contraire à son dernier terme, et une équation de degré pair à une racine positive et une racine négative au moins, si son dernier terme est négatif.*

Théorème de Descartes.

104. Lorsque deux termes consécutifs d'une équation ont le même signe, on dit qu'ils forment une permanence; lorsqu'ils ont des signes contraires, ils forment une variation.

Descartes a démontré le théorème suivant :

Une équation ne saurait avoir plus de racines positives que de variations, ni plus de racines négatives que de permanences.

Pour démontrer ce théorème, nous considérerons une équation quelconque ordonnée suivant les puissances décroissantes de x, et en la multipliant par $x - a$, nous introduirons la racine positive a. Nous allons voir que, quels que soient les signes des termes, cette multiplication introduit une variation au moins.

Le premier terme x^n de l'équation peut être censé positif; la première variation se rencontre dès que l'on arrive à un terme négatif et, comme il est précédé d'un terme positif, ces deux termes seront

$$a_{n-p}x^p - a_{n-p+1}x^{p-1}.$$

Un des termes de la nouvelle équation sera alors

$$-(aa_{n-p} + a_{n-p+1})x^p.$$

On ignore si le terme précédent est positif, mais ce que l'on sait, c'est qu'il existe au moins un terme précédent positif et si, par suite, on parcourt la suite des termes depuis le premier jusqu'au terme en x^p, on rencontrera au moins une variation, comme dans la première équation à x^{p-1}. Si, en parcourant la suite des termes jusqu'au terme en x^p, on rencontre plus d'une variation, on en rencontrera évidemment un nombre impair, car le changement d'un signe ne peut jamais produire une augmentation ou diminution d'un nombre impair de variations.

La première variation que l'on rencontre ensuite se trouve

quand on parvient à un terme positif. Supposons que ce terme soit en x^q, on montrera, comme tout à l'heure, que le terme en x^{q+1} dans la nouvelle équation est positif, de sorte que, quels que soient les signes précédents, il y a, entre x^p et x^{q+1}, au moins une variation dans la nouvelle équation; en continuant ainsi on verra qu'en arrivant au terme x^r dans l'ancienne équation, et au terme x^{r+1} dans la nouvelle, on a, dans cette dernière, rencontré au moins autant de variations que dans la première. Supposons que, après avoir passé par le terme en x^r dans la première équation, on ne rencontre plus de variations, soit $\pm k$ le coefficient de x^r, tous les termes qui suivent ont le signe de k; dans la nouvelle équation, le terme en x^{r+1} a le signe de k, tandis que le dernier terme est $-aa_n$, qui est de signe contraire à k. Si donc on parcourt la suite des termes à partir de x^{r+1}, on rencontre encore au moins une variation dans la nouvelle équation; comme la suite des termes jusqu'à x^{r+1} (inclus) présentait au moins autant de variations que dans l'ancienne équation, il faut nécessairement que la nouvelle équation présente au moins une variation de plus que l'ancienne.

Supposons maintenant que l'on ait divisé le premier membre de $f(x) = 0$ par tous les facteurs linéaires qui correspondent aux racines positives; l'équation que l'on obtient n'a plus que les racines négatives et imaginaires de l'ancienne équation; et l'on ne sait rien sur le nombre de ses variations. Réintroduisons successivement les facteurs que l'on avait supprimés, à chaque fois on introduit au moins une nouvelle variation.

Quand on a réintégré toutes les racines positives, on retombe sur l'équation primitive, qui doit avoir autant de variations au moins que de racines positives. En changeant x en $-x$, on établit la seconde partie du théorème.

Le nombre total des variations et des permanences d'une équation de degré n est précisément n. *Si donc cette équation a toutes ses racines réelles, le nombre des variations est égal au nombre des racines positives, le nombre des permanences est égal au nombre des racines négatives.*

Si un ou plusieurs coefficients sont nuls, on peut les regarder à volonté comme positifs ou négatifs, une variation infiniment petite dans un coefficient ne pouvant changer le signe d'une racine (en faisant abstraction du cas où l'équation a une racine nulle). On peut donc, quand il y a des termes nuls, les remplacer par d'autres choisis de manière à rendre minimum le nombre des variations et des permanences. Si l'on a un terme nul entre deux de signes contraires, on peut le supposer positif ou négatif à volonté, car

$$+ \; 0 \; -$$

donne une variation et une permanence, quel que soit le signe que l'on mette à la place de o. Si, au contraire, il se trouve un terme nul entre deux de mêmes signes, l'équation a au moins deux racines imaginaires; car, si l'on a

$$+ \; 0 \; +,$$

on peut, pour compter le nombre des variations, supposer que l'on a

$$+ \; + \; +,$$

et, pour compter le nombre des permanences, supposer que l'on a

$$+ \; - \; +;$$

la somme du nombre des variations et du nombre des permanences sera donc de deux unités moindres au moins que le degré de l'équation, ce qui montre qu'elle a au moins deux racines imaginaires.

Lorsque la somme du nombre des variations et du nombre des permanences n'est pas égale au nombre des racines réelles la différence est un nombre pair; cela résulte de ce que l'introduction d'une racine positive correspond à l'introduction d'un nombre impair de variations, et à ce qu'une équation qui n'a que des racines imaginaires a un nombre pair de variations (son dernier terme est positif).

Exemple :

$$x^7 + x^5 - x^4 - 2x^3 - x + 1 = 0.$$

On peut lire

$$+ + + - - - - +$$

ou

$$+ - + - - + - +$$

et l'équation a au plus deux racines positives et une racine négative; elle a donc au moins quatre racines imaginaires.

Théorème de Budan.

105. Les théorèmes de Descartes et de Newton sont des cas particuliers d'un théorème de Budan; ce théorème a aussi été donné par Fourier, qui l'a développé dans ses leçons; mais il a été publié avant par Budan.

Considérons la suite

$$f(x),\quad f'(x),\quad f''(x),\quad \ldots,\quad f^{(n)}(x),$$

et substituons à la place de x les nombres a, b où $a < b$.

L'équation $f(x) = 0$ n'a pas plus de racines entre a et b que de variations perdues par la suite précédente, quand on passe de a à b.

On voit facilement que quand l'une des fonctions de la suite passe par zéro, la précédente et la suivante sont de signes contraires; si l'on considère $f^{(p)}(x)$, par exemple, on a

$$f^{(p)}(x - h) = f^{(p)}(x) - f^{(p+1)}(x)h + \ldots,$$
$$f^{(p)}(x + h) = f^{(p)}(x) + f^{(p+1)}(x)h + \ldots;$$

pour $f^{(p)}(x) = 0$ et pour h infiniment petit

$$f^p(x - h) \quad \text{et} \quad f^{p+1}(x)$$

ont des signes contraires; $f^{p+1}(x)$ et $f^p(x + h)$ ont le même signe si $f^{(p)}(x)$ et $f^{(p+1)}(x)$ ne sont pas nuls à la fois. Si donc deux dérivées consécutives ne sont pas nulles en même temps, il faut qu'il se perde une variation quand x traverse une racine de la première. Si l'on considère alors la suite

$$f^{(p-1)}(x),\quad f^{(p)}(x),\quad f^{(p+1)}(x),$$

on voit que si $f^{(p)}(x)$ s'annule, il se perdra une variation par les deux dernières fonctions, tandis que par les deux premières il se gagnera ou se perdra une variation ; ainsi quand $f^{(p)}(x)$ s'annule, il se perd deux ou zéro variations; quand $f(x)$ s'annule, il se perd toujours une variation, puisqu'il n'existe aucune fonction avant. On arrive ainsi au résultat suivant : *Il se perd au moins une variation chaque fois que l'on passe par une racine de l'équation $f(x) = 0$, il peut s'en perdre plus qu'il n'y a de racines, mais l'excès est pair.*

106. Il faut examiner le cas particulier où plusieurs fonctions consécutives s'annulent; soit $f^{(p-1)}(x)$ la dernière d'entre elles; on a

$$f^{(p-1)}(x-h) = -f^{(p)}(x)\ h\ +\ldots,\quad f^{(p-1)}(x+h) = f^{(p)}(x)\ h\ +\ldots,$$

$$f^{(p-2)}(x-h) = +f^{(p)}(x)\ \frac{h^2}{1.2}\ +\ldots,\quad f^{(p-2)}(x+h) = f^{(p)}(x)\ \frac{h^2}{1.2}\ +\ldots,$$

$$f^{(p-3)}(x-h) = -f^{(p)}(x)\ \frac{h^3}{1.2.3}+\ldots,\quad f^{(p-3)}(x+h) = f^{(p)}(x)\ \frac{h^3}{1.2.3}+\ldots,$$

. . . .

Les fonctions qui s'annulent à la fois présentent, avant le passage par zéro, uniquement des variations et, après le passage, elles ne présentent que des permanences ; de sorte que, dans ce cas, il y a encore perte de variations. Dans le cas particulier où les p premières fonctions s'annulent l'équation a p racines égales et il se perd alors p variations. Le théorème est donc applicable à tous les cas et, en particulier, aux racines multiples.

Si l'on pose $x = -\infty$, la suite n'a que des variations; si l'on fait $x = 0$, on obtient les signes des coefficients de l'équation; si l'on fait $x = +\infty$, on n'a plus que des permanences. C'est justement le théorème de Descartes, qu'on obtient ici comme cas particulier du théorème de Budan.

Si l'on remplace x par un nombre k qui ne donne que des permanences, il n'y aura pas de racines entre k et ∞; k sera donc une limite supérieure des racines ; de sorte que le théorème de Newton est aussi contenu dans celui de Budan.

Si $f(a)$ et $f(b)$ sont de signes contraires, tous les autres termes de la suite conservant les mêmes signes pour $x=a$ et $x=b$, *il n'y a qu'une racine entre a et b*, car on a vu qu'entre a et b il y a un nombre impair de racines, et il n'y a eu qu'une variation perdue. Dans ce cas la racine est séparée par a et b, il faut cependant remarquer que la séparation ne pourra pas toujours se faire par ce procédé, parce que plusieurs fonctions de la suite peuvent s'annuler avec $f(x)$, et qu'il peut ainsi se perdre à la fois plusieurs variations.

Au moyen de la suite considérée, on peut se procurer une limite supérieure du nombre des racines comprises entre deux nombres donnés, mais la considération de la suite ne permet pas d'affirmer l'existence de racines imaginaires, car de $-\infty$ à $+\infty$ il se perd toujours le même nombre de variations, que l'équation ait ou n'ait pas de racines imaginaires.

Théorème de Rolle.

107. *Si a et b sont deux racines consécutives de l'équation $f(x)=0$, l'équation $f'(x)=0$ a au moins une racine comprise entre a et b, en tout cas un nombre impair de racines comprises entre ces limites.*

Puisque $f(x)$ est une fonction continue, comme elle s'annule pour $x=a$ et $x=b$, elle ne peut aller sans cesse en croissant ou sans cesse en décroissant; elle doit donc passer par un maximum ou un minimum pour une valeur de x comprise entre a et b et cette valeur est racine de $f'(x)=0$.

La fonction peut avoir plusieurs maxima ou minima, mais comme elle ne s'annule pas entre a et b, il faut bien, si elle commence par croître, qu'elle finisse par décroître ou, si elle commence par décroître, qu'elle finisse par croître; il est facile de voir qu'il en résulte un nombre impair de maxima ou de minima. La considération de la courbe $y=f(x)$ rend ces développements évidents.

Il résulte de là qu'entre deux racines consécutives de $f'(x)=0$, il ne peut y avoir plus d'une racine de $f(x)=0$;

car s'il y en avait deux, entre celles-ci il y aurait une racine de $f'(x)=0$. Il en résulte que, *quand* $f(x)=0$ *a toutes ses racines réelles*, $f'(x)$ *a aussi toutes ses racines réelles; que si* $f(x)$, *pour* $x=a$, *a* p *racines égales*, $f'(x)=0$, *pour cette même valeur, a* $p-1$ *racines égales.*

Exemple :

$$f(x) = x^m + px^n + q = 0 \qquad (m \text{ et } n \text{ sont impairs}).$$

La règle de Descartes montre que l'équation a une ou trois racines réelles. Or

$$f'(x) = mx^{n-1}\left(x^{m-n} + \frac{np}{m}\right).$$

1° Si p *est positif*, $f'(x)$ n'a d'autre racine réelle que $x=0$: donc $f(x)=0$ n'a qu'une racine réelle;

2° p *est négatif*. $f'(x)=0$ a une racine nulle et deux autres racines réelles : appelons-les $-b$ et $+b$; $f(x)=0$ peut avoir trois racines réelles dans les intervalles ($n-1$ est pair) :

$$-\infty, \qquad -b, \qquad +b, \qquad +\infty,$$

ces valeurs, portées dans $f(x)$, donnent les signes

$$- \quad + \quad - \quad +,$$

si les trois racines réelles existent; pour qu'il en soit ainsi il faut que

$$-b^m - pb^n > -q,$$

ou, en remplaçant b par sa valeur et en simplifiant,

$$\left(\frac{nq}{m-n}\right)^{m-n} + \left(\frac{np}{m}\right)^m < 0.$$

La condition pour que

$$x^3 + px + q = 0$$

ait trois racines réelles est

$$4p^3 + 27q^2 < 0.$$

Théorème de Sturm.

108. Nous avons remarqué que ce qui empêchait le théorème de Budan de donner le nombre exact des racines réelles comprises dans un intervalle, c'est que lorsqu'un terme de la suite s'annule il peut se perdre des variations, sans que $f(z)$ passe par zéro. Sturm a tourné cette difficulté en faisant usage d'une autre suite qui jouit de cette propriété que, lorsqu'un terme de la suite s'annule, ceux qui le comprennent sont de signes contraires de sorte que le nombre de variations n'est pas altéré quand un terme intermédiaire de la suite passe par zéro. La suite de Sturm a pour premiers termes, comme celle de Budan, $f(x)$ et $f'(x)$; les autres termes sont les restes que l'on obtient en appliquant à ceux-ci la méthode du plus grand commun diviseur en ayant soin de changer chaque fois les signes de ces restes et en n'introduisant que des facteurs positifs pour éviter les fractions. Nous supposerons l'équation débarrassée de ses racines multiples : $f(x)$ et $f'(x)$ n'auront pas alors de facteurs communs et le dernier reste sera indépendant de x; les termes de la suite sont donc $f(x)$, $f'(x)$ et les restes changés de signes; nous les désignerons par

$$f(x),\quad f'(x),\quad f_2(x),\quad f_3(x),\quad \ldots,\quad f_n(x);$$

alors, en désignant par un q les quotients et par un c des facteurs positifs,

$$\begin{aligned}
c\,f(x) &= q\,f'(x) - f_2(x),\\
c_1 f'(x) &= q_1 f_2(x) - f_3(x),\\
c_2 f_2(x) &= q_2 f_3(x) - f_4(x),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
c_{n-2} f_{n-2}(x) &= q_{n-2} f_{n-1}(x) - f_n(x).
\end{aligned}$$

Ces restes donnent lieu aux remarques suivantes :

Deux termes consécutifs de la suite $f(x)$, $f'(x)$, $f_2(x)$, ... ne peuvent s'annuler pour une même valeur de x.

En effet, s'il en était ainsi, tous les restes, jusqu'au dernier, seraient nuls, et l'équation aurait des racines égales.

Si un terme de la suite [excepté $f(x)$] s'annule, celui qui le précède et celui qui le suit sont de signes contraires.

Par exemple, pour $f_3(x)=0$, on a $c_2 f_2(x)=-f_4(x)$. Si l'on fait varier x de $-\infty$ à $+\infty$, les termes de la suite ne pourront changer de signe qu'en passant par zéro; donc il ne se perdra pas de variation, puisque, quand un terme s'annule, celui qui le précède et celui qui le suit sont de signes contraires, de sorte que, avant comme après le passage par zéro, les trois termes considérés forment une variation et une permanence. Cette conclusion ne s'applique pas au premier et au dernier terme de la suite, qui n'en ont pas avant ou après eux. Mais le dernier terme est indépendant de x et ne saurait changer de signe et, en vertu de ce qui a été dit (105), il se perd une variation quand $f(x)$ change de signe. La suite considérée perd donc une variation toutes les fois que x passe par une racine de $f(x)=0$. Ainsi :

Si, dans la suite de Sturm, on fait $x=a$ et $x=b$, le nombre des variations perdues est égal au nombre des racines comprises entre a et b ($b>a$).

Quand la valeur substituée annule un terme de la suite de Sturm, suivant le premier, on peut le supposer égal à $+0$ ou à -0. Si le premier terme est nul, c'est une racine de l'équation, et si l'on veut le faire entrer dans la suite, il faudra faire commencer cette suite par une variation ou une permanence, suivant que la racine en question sera une limite supérieure ou une limite inférieure de l'intervalle considéré.

Lorsqu'un terme de la suite de Sturm ne change pas de signe dans l'intervalle considéré, on peut arrêter la suite à ce terme. En effet, la démonstration du théorème de Sturm suppose seulement que le dernier terme de la suite conserve toujours le même signe, et il est indifférent que ce terme soit ou non fonction de x.

109. Quand on forme la suite de Sturm, on trouve le plus grand commun diviseur de $f(x)$ et $f'(x)$, qu'il y ait ou qu'il n'y ait pas de racines multiples; s'il y a des racines multiples, tous les termes de la suite acquièrent un facteur commun φ, il peut être écarté par une division, sans que les propriétés de la suite cessent d'avoir lieu : le dernier terme est alors constant, les deux premiers $\frac{f(x)}{\varphi}$ et $\frac{f'(x)}{\varphi}$ perdent une variation quand $f(x)$ et $f'(x)$ s'annulent; et, après la division, un terme qui s'annule se trouve toujours entre deux autres de signes contraires; donc, après la division, on peut encore appliquer le théorème de Sturm, mais *les racines multiples ne peuvent être comptées qu'une fois*. On n'a pas besoin de diviser par le facteur φ, car, s'il est positif, il ne change pas les signes de la suite; s'il est négatif, il les change tous; en aucun cas, le nombre des variations ne se trouve changé.

Si l'équation donnée est de degré n et a toutes ses racines réelles, la suite de Sturm a $n+1$ termes; pour $x=-\infty$, elle ne doit avoir que des variations; pour $x=+\infty$, elle ne doit avoir que des permanences, et il faut pour cela que tous les termes de la suite aient leur premier coefficient positif.

En posant $x=-\infty$ et $x=0$ dans la suite de Sturm, on a le nombre des racines négatives; en posant $x=0$ et $x=\infty$, on a le nombre des racines positives. Les racines manquantes sont imaginaires.

Exemple I :

$$x^6+3x^4-4x^3+6x^2+12x-18=0,$$

	$-\infty$.	$+\infty$.	o.
$f(x)=x^6+3x^4-4x^3+6x^2+12x-18$ ...	+	+	—
$\frac{1}{6}f'(x)=x^5+2x^3-2x^2+2x+2$	—	+	+
$f_2(x)=-x^4+2x^3-4x^2-10x+18$.......	—	—	+
$f_3(x)=-x^3+10x^2-19$.................	+	—	—
$f_4(x)=84x^2-9x-170$....................	+	+	—
$f_5(x)=2267x-2402$........................	—	+	—
$f_6(x)=+$....................................	+	+	+

Pour $x = -\infty$, on a quatre variations; pour $x = 0$, on en a trois; et pour $x = +\infty$, on en a deux. L'équation a donc une racine négative, une racine positive et quatre racines imaginaires.

Exemple II :

$$x^3 + ax + b = 0,$$
$$f(x) = x^3 + ax + b,$$
$$f'(x) = 3x^2 + a,$$
$$f_2(x) = -2ax - 3b,$$
$$f_3(x) = -4a^3 - 27b^2.$$

La condition, pour que l'équation ait trois racines réelles, est que a soit négatif et que

$$4a^3 + 27b^2 < 0.$$

La première condition est comprise dans la seconde; si elle est remplie, on a, pour $x = 0$,

$$b, \quad a, \quad -3b, \quad + \ldots.$$

Les trois premiers termes donnent toujours une permanence et une variation; on a deux racines positives et une racine négative quand b est positif, deux racines négatives et une positive quand b est négatif.

On rencontre souvent des suites de fonctions qui jouissent des propriétés caractéristiques des suites de Sturm, et l'on peut en profiter pour déterminer la nature des racines des équations obtenues en égalant ces fonctions à zéro; les exemples suivants mettront ce fait en évidence :

1° Dans la fraction continue suivante, où a_1, a_2, ... sont positifs,

$$\cfrac{1}{x - \cfrac{a_1}{x - \cfrac{a_2}{x - \cdots}}},$$

les dénominateurs des réduites sont liés entre eux par les relations

$$Q_{n+1} = xQ_n - a_{n-1}Q_{n-1}, \qquad Q_0 = 1, \qquad Q_1 = x.$$

On voit facilement que le premier terme de Q_n est x^n et que la suite

$$Q_n, \quad Q_{n-1}, \quad \ldots, \quad x, \quad 1$$

jouit des propriétés de la suite de Sturm. Comme le second terme n'est pas la dérivée du premier, on ne peut pas en conclure qu'une variation se perd toutes les fois que le premier terme passe par zéro, mais dans le passage de $-\infty$ à $+\infty$, on perd n variations. Q_n a donc dû s'annuler n fois et, comme il est du degré n, $Q_n = 0$ a toutes ses racines réelles.

Les théorèmes suivants se démontrent de la même façon.

2° La $n^{\text{ième}}$ dérivée de la fonction

$$\frac{1}{1+x^2}$$

est de la forme

$$\frac{P_n}{(1+x^2)^{n+1}};$$

l'équation $P_n = 0$ a toutes ses racines réelles.

3°

$$\frac{1}{1+2\alpha x+\alpha^2} = U_0 + U_1\alpha + U_2\alpha^2 + \ldots;$$

l'équation $U_n = 0$ a toutes ses racines réelles.

4° La $n^{\text{ième}}$ dérivée de e^{-x^2} est de la forme $P_n e^{-x^2}$; l'équation $P_n = 0$ a toutes ses racines réelles. (Hermite.)

5°

$$u = (1 - 2\alpha x + \alpha^2)^{-\frac{1}{2}} = u_0 + u_1\frac{\alpha}{1} + u_2\frac{\alpha^2}{1.2} + \ldots;$$

les polynomes u_0, u_1, u_2, ... sont appelés polynomes de Legendre. $u_n = 0$ a toutes ses racines réelles; on trouve, en effet, en différentiant par rapport à α,

$$u - 3(x-\alpha)u' + (1 - 2\alpha x + \alpha^2)u'' = 0,$$

et en différentiant plusieurs fois de suite, puis en faisant $\alpha = 0$,

$$u_n = (2n-1)x u_{n-1} - (n-1)^2 u_{n-2}, \qquad u_0 = 1, \qquad u_1 = x,$$

on peut terminer la suite à l'unité.

Application du théorème de Sturm aux racines imaginaires.

110. On a vu plus haut que si, dans une équation à coefficients réels ou imaginaires

$$f(z) = 0,$$

on posait

$$z = x + yi,$$

elle se partageait en deux autres

$$A = 0, \qquad B = 0,$$

qui pouvaient être regardées comme les équations de deux courbes dont les intersections étaient les points représentant les racines de l'équation. Nous allons nous proposer de trouver le nombre des points racines contenus dans un contour fermé. Pour plus de simplicité, nous supposerons qu'il s'agisse de trouver le nombre des racines contenues à l'intérieur d'un cercle de rayon r et dont le centre a pour coordonnées a et b. L'équation de ce cercle peut être remplacée par les deux suivantes :

$$x = a + r\frac{1 - t^2}{1 + t^2}, \qquad y = b + r\frac{2t}{1 + t^2},$$

qui, par l'élimination de t, donnent l'équation du cercle.

La circonférence du cercle est parcourue dans un sens déterminé quand on fait varier t de $-\infty$ à $+\infty$. En vertu du théorème de Cauchy, le nombre des points racines contenus à l'intérieur du cercle est la moitié de la différence du nombre de fois que AB passe du négatif au positif et du positif au négatif. Ces nombres sont les mêmes que celui de changements des variations que présentent A et B écrits l'un après l'autre, ou des permanences qu'ils présentent.

Remplaçons maintenant x et y par leurs valeurs en t, et multiplions A et B par un même facteur, de manière à les changer en deux polynomes entiers en t et premiers entre eux.

Opérons ensuite sur ces polynomes comme on l'a fait plus haut sur $f(x)$ et $f'(x)$, on obtiendra une série de polynomes. Cherchons combien il se perd de variations dans cette suite quand on fait varier t de $-\infty$ à $+\infty$. Comme la suite ne peut perdre de variations que par son premier terme, chaque terme étant compris entre deux autres de signes contraires quand il s'annule, le nombre de variations perdues donnera la différence du nombre de fois que le produit des deux premiers termes passera du négatif au positif et du positif au négatif, et comme ces deux premiers termes ne diffèrent de A et B que par un même facteur, leur produit a le signe de AB. On voit ainsi que, *pour chaque racine contenue à l'intérieur du cercle, il se perd deux variations* (*ou il s'en gagne deux*).

Séparation des racines réelles.

111. D'après ce que l'on a vu, il est facile de voir si, entre deux nombres donnés, il y a un nombre pair ou impair de racines réelles. Mais, avant de procéder au calcul numérique des racines, il faut déterminer des intervalles qui ne comprennent qu'une racine. Il y a des cas particuliers où il est très facile de séparer une racine; par exemple quand tous les termes sont positifs, sauf le dernier, l'équation n'a qu'une racine positive, et celle-ci se trouve séparée. Si l'on remplace x par 1, 10, 100, ..., on peut déterminer deux de ces nombres comprenant la racine; on peut ensuite resserrer les limites jusqu'à ce que l'on ait renfermé la racine entre deux nombres entiers; on abrège le nombre des essais en déterminant une limite supérieure et une limite inférieure des racines.

Une méthode très sûre, mais très pénible pour la séparation des racines, a été donnée par Waring et, plus tard, par Lagrange; elle consiste à former l'équation aux carrés des différences des racines et à déterminer une limite inférieure de ses racines positives; soit α cette limite; entre deux racines quelconques de l'équation proposée, on aura

$$x_p - x_q > \sqrt{\alpha};$$

si l'on forme alors la suite

$$\sqrt{\alpha}, \quad 2\sqrt{\alpha}, \quad 3\sqrt{\alpha}, \quad \ldots,$$

deux termes consécutifs de cette suite ne pourront comprendre plus d'une racine, car, s'il en était autrement, la différence de deux racines serait moindre que $\sqrt{\alpha}$.

Cette méthode suppose, bien entendu, l'équation débarrassée de ses racines multiples, sans quoi l'on trouverait $\alpha = 0$.

On peut, toutefois, modifier la méthode de manière à n'avoir besoin de connaître que le dernier terme de l'équation aux carrés des différences; nous ne nous arrêterons pas davantage sur cette méthode, parce que le théorème de Sturm permet plus facilement la séparation des racines.

Pour séparer les racines, on forme la suite de Sturm et l'on remplace x successivement par des valeurs entre lesquelles on en intercale de nouvelles, jusqu'à ce que l'on parvienne à deux valeurs telles que, en passant de l'une à l'autre, la suite de Sturm ne perde plus qu'une variation. Les racines sont ainsi complètement séparées, et l'on peut, par de simples essais, resserrer l'intervalle comprenant une racine.

Exemple :

$$x^4 + x^3 - 4x^2 - 4x + 1 = 0.$$

La suite de Sturm est

	$+\infty$.	-2.	-1.	0.	$+1$.	$+2$.
$x^4 + x^3 - 4x^2 - 4x + 1$	+	+	+	+	—	+
$4x^3 + 3x^2 - 8x - 4$	—	—	+	—	—	+
$7x^2 + 8x - 4$	+	+	—	—	+	+
$4x + 5$	—	—	+	+	+	+
+	+	+	+	+	+	+

Ce Tableau montre que, dans le passage de -2 à -1, de 0 à 1, de 1 à 2, il se perd respectivement 2, 1 et 1 variations; l'équation a donc quatre racines réelles, les racines positives se trouvent séparées; pour séparer celles qui sont comprises

entre -2 et -1, on fera $x = -\frac{3}{2}$ dans le premier membre de l'équation proposée, et l'on obtiendra un résultat négatif; il en résulte qu'une des racines négatives est comprise entre -1 et $-1,5$, et l'autre entre $-1,5$ et -2.

Méthode de Fourier.

112. Le théorème de Sturm permet de séparer à coup sûr les racines, mais les calculs auxquels conduit cette méthode sont très prolixes. Une équation du sixième ou du septième degré avec des coefficients très simples conduit ordinairement à des résultats contenant cinquante chiffres et plus; aussi, dans la pratique, est-il souvent plus commode de faire usage du théorème de Budan.

On se souvient que la suite de Budan est

$$f(x),\quad f'(x),\quad f''(x),\quad \ldots,$$

et l'on fait usage de cette suite comme de celle de Sturm; mais le nombre des variations perdues ne donne qu'une limite supérieure des racines comprises dans l'intervalle correspondant. Ainsi il peut se perdre deux variations quand un terme intermédiaire de la suite s'annule, sans pour cela que $f(x)$ passe par zéro; cela arrive quand le terme nul est placé entre deux autres de même signe. Comme en passant de $-\infty$ à $+\infty$ on perd n variations quand l'équation est de degré n, l'équation a deux racines imaginaires toutes les fois qu'il se perd deux variations par suite du passage par zéro d'une des fonctions $f'(x)$, $f''(x)$.... On peut donc conclure de là que si, x variant de a à b, la suite de Budan ne perd pas de variations, l'équation n'a pas de racine comprise entre a et b et que, si elle en perd une, il y a une racine entre a et b. Si elle en perd deux, ou bien l'équation a deux racines imaginaires, ou bien elle a deux racines réelles comprises entre a et b.

113. Supposons que l'on ait trouvé un intervalle dans lequel il se perde deux variations, et cela entre les trois pre-

miers termes; alors, en supposant $f(x)$ positif pour les deux limites α et $\beta\,(\beta > \alpha)$, on aura

$$\begin{array}{cccccc} f(\alpha), & f'(\alpha), & f''(\alpha), & f(\beta), & f'(\beta), & f''(\beta), \\ + & - & + & + & + & + \end{array}$$

Si nous supposons qu'il ne se soit pas perdu de variations dans le reste de la suite, $f''(x) = 0$ n'a pas de racine entre α et β. $f''(x)$ est donc toujours positif dans l'intervalle; si $f(x)$ reste également positif, la perte de deux variations doit indiquer l'existence de deux racines imaginaires. Des considérations géométriques vont nous permettre de nous rendre compte de ce qui arrive en général.

Comme les intersections de la courbe

$$y = f(x)$$

avec l'axe des x donnent les racines de l'équation $f(x) = 0$, il s'agit de trouver si entre $x = \alpha$ et $x = \beta$ il existe deux ou zéro points d'intersection. Comme $f'(x)$ change de signe tandis que $f''(x)$ conserve son signe dans l'intervalle considéré, il doit y avoir dans cet intervalle un minimum et la concavité est tournée vers le haut; les deux cas sont représentés par les *fig.* 7 et 8.

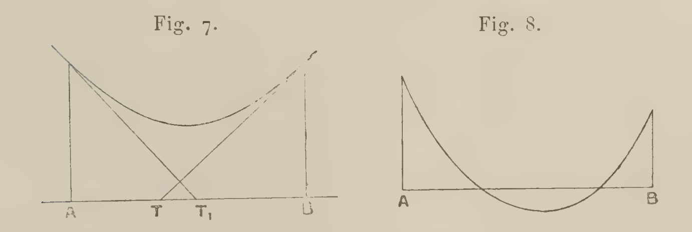


Fig. 7. Fig. 8.

La première correspond au cas où il y a deux racines imaginaires, la seconde au cas où il y a deux racines réelles. Si les tangentes aux points limites se coupent au-dessus de l'axe des x, il y a nécessairement des racines imaginaires, mais la réciproque n'est pas vraie. On peut seulement dire

qu'il y a des racines imaginaires si

$$AT_1 + TB \geqq AB,$$

ou

$$\frac{f(\beta)}{f'(\beta)} - \frac{f(\alpha)}{f'(\alpha)} \geqq \beta - \alpha. \tag{1}$$

Je répète que, de ce que les tangentes ne se coupent pas au-dessus de l'axe des x, il ne faut pas conclure à l'existence des racines réelles, mais on voit que, si les racines sont imaginaires, on pourra toujours rapprocher les limites α et β pour que l'intersection des tangentes ait lieu au-dessus de l'axe des x. On resserrera alors l'intervalle compris entre α et β jusqu'à ce que la relation (1) soit satisfaite, ou jusqu'à ce que la perte de deux variations soit remplacée par la perte d'une variation; dans le premier cas, on est en présence de deux racines imaginaires; dans le second, on est en présence de deux racines réelles.

114. Maintenant, nous allons examiner le cas où, dans le passage de α à β, la série perd d variations.

Laissons de côté le terme $f(x)$, c'est-à-dire considérons $f'(x) = 0$ comme l'équation donnée, alors on perdra d_1 variations; en considérant $f''(x) = 0$ comme l'équation donnée, on en perdra d_2, etc. Deux d consécutifs sont alors égaux ou différents d'une unité, Fourier appelle d_p l'indice de $f^{(p)}(x)$.

Maintenant, considérons le premier indice de la série qui a pour valeur 1; soit d_p cet indice, $f^{(p)}(x) = 0$ a alors une racine entre α et β; l'indice précédent doit être 2, car, s'il était égal à zéro, il devrait y avoir un indice antérieur égal à 1; l'indice suivant peut être 2, 1 ou 0; s'il est 2 ou 1, on peut toujours subdiviser l'intervalle, de telle sorte que l'intervalle qui contient la racine de $f^{(p)}(x) = 0$ ne contienne pas de racine de $f^{(p+1)}(x) = 0$; pour les autres intervalles, on a

$$d_p = 0,$$

et le premier indice 1 est à chercher plus à gauche dans la

suite; donc on n'a besoin de considérer que le cas où

$$d_{p-1} = 2, \qquad d_p = 1, \qquad d_{p+1} = 0;$$

ce cas est celui que nous avons examiné (**113**), et l'on peut décider si les racines de

$$f^{(p-1)}(x) = 0$$

sont réelles ou imaginaires; si elles sont réelles, on peut scinder l'intervalle en deux autres, contenant chacun une racine et, comme chacun a l'indice 1, on peut continuer de la même façon; si elles sont imaginaires, les deux variations doivent être perdues et quand une fonction suivante s'annule elle doit se trouver entre deux autres de même signe.

L'équation proposée doit donc aussi avoir deux racines imaginaires; si l'on en fait abstraction, on peut retrancher 2 de chacun des indices de la partie de la suite qui reste à étudier. Si l'on continue de cette manière, on peut rejeter le premier indice 1 vers un terme moins avancé dans la suite, et, quand on l'a ramené jusqu'au premier terme, la racine est séparée.

Exemple :

$$x^5 - 5x^4 - 16x^3 + + 12x^2 - 9x - 5 = 0.$$

On a

$$f(x) = x^5 - 5x^4 - 16x^3 + 12x^2 - 9x - 5,$$

$$f'(x) = 5x^4 - 20x^3 - 48x^2 + 24x - 9,$$

$$\frac{1}{4} f''(x) = 5x^3 - 15x^2 - 24x + 6,$$

$$\frac{1}{12} f'''(x) = 5x^2 - 10x - 8,$$

$$\frac{1}{120} f^{\text{iv}}(x) = x - 1,$$

$$f^{\text{v}}(x) \quad +;$$

la limite supérieure des racines est 8. Dans l'intervalle 0, 8 on perd trois variations; deux de 0 à 1, une de 7 à 8. Il y a donc une racine entre 7 et 8 qui se trouve séparée. L'inter-

valle de o à 1 doit être examiné de plus près; les signes de la suite sont

$$\text{Pour } x = 0: \quad - \; - \; + \; - \; - \; +,$$
$$\text{»} \quad x = 1: \quad - \; - \; - \; - \; - \; +,$$

si l'on regarde o comme négatif; alors on a

$$d_1 = 2, \quad d_2 = 1, \quad d_3 = 0,$$

et

$$\frac{f'(1)}{f''(1)} - \frac{f'(0)}{f''(0)} = \frac{3}{7} + \frac{3}{8} < 1;$$

il faut alors resserrer les limites; on pose $\beta = \frac{1}{2}$ et l'on a les signes

$$- \; - \; - \; - \; - \; +;$$

les variations se perdent donc de o à $\frac{1}{2}$; on trouve alors

$$\frac{f'\left(\frac{1}{2}\right)}{f''\left(\frac{1}{2}\right)} - \frac{f'(0)}{f''(0)} > \frac{1}{2};$$

d'où il résulte que les deux racines sont imaginaires. L'équation a encore deux racines négatives, l'une entre — 3 et — 2, l'autre entre — 1 et o.

115. Les racines imaginaires peuvent être séparées par la méthode donnée (110), ou encore en remplaçant le cercle par deux parallèles à l'axe des y, qui servent à séparer les parties réelles, ou par deux parallèles à l'axe des x, qui servent à séparer les coefficients de i.

Théorème de Newton.

116. Newton a énoncé sans démonstration un théorème établi plus tard par Sylvester et généralisé par lui et qui corrige les indications du théorème de Budan, relatif au nombre des racines comprises entre deux limites données.

On considère une seconde suite dont tous les termes sont conjugués deux à deux avec celle de Budan. Lorsque dans la série de Budan on a une variation, les termes de la série conjuguée formant une permanence, nous dirons que nous avons une *variation-permanence* et nous désignerons cette circonstance par le symbole V-P; l'équation $f(x)=0$ étant de degré n, les deux suites sont

$$(1)\quad \left\{\begin{array}{ll} f(x), & f^2(x), \\ f'(x), & [f'(x)]^2-k_1 f(x) f''(x), \\ f''(x), & [f''(x)]^2-k_2 f'(x) f'''(x), \\ \cdots\cdots & \cdots\cdots\cdots\cdots\cdots, \\ f^{(p)}(x), & [f^{(p)}(x)]^2-k_p f^{(p-1)}(x) f^{(p+1)}(x), \\ \cdots\cdots & \cdots\cdots\cdots\cdots\cdots \end{array}\right.$$

où

$$(2)\qquad k_p=\frac{n-p+1}{n-p}.$$

Pour abréger, nous désignerons $f^{(p)}(x)$ par f_p.

Nous allons étudier les changements des V-P que l'on rencontre dans la double suite quand on fait croître x; il faut remarquer que

$$(3)\qquad 2-k_p=\frac{1}{k_{p+1}}.$$

Nous supposerons d'abord que deux termes consécutifs ne s'annulent pas en même temps.

Le nombre des V-P ne peut changer que quand un terme de l'une des deux suites passe par zéro.

Supposons que ce soit le cas pour f_p, le changement s'opérera entre les termes

$$\begin{array}{ll} f_{p-1}, & f_{p-1}^2-k_{p-1} f_{p-2} f_p, \\ f_p, & f_p^2 \;\; -k_p \;\; f_{p-1} f_{p+1}, \\ f_{p+1}, & f_{p+1}^2-k_{p+1} f_p \;\; f_{p+2}; \end{array}$$

pour $f_p=0$ les signes des termes de la seconde suite sont

$$+,\quad \pm,\quad +.$$

Si le signe du milieu est $+$ on a une V-P, c'est-à-dire si f_{p-1} et

f_{p+1} sont de signes contraires; dans ce cas, dans la première suite, il y a une variation et une permanence, de sorte que, dans les trois paires de termes, il y a une V-P avant comme après l'annulation de f_p.

Ceci n'a plus lieu quand c'est $f(x)$ qui s'annule; dans la première suite une variation se change en permanence et les deux premiers termes de la seconde série sont positifs et forment une permanence; donc, en tout cas, il se perdra une V-P quand x passera par une racine de $f(x) = 0$, pendant qu'il ne se produit aucun changement dans les V-P quand un autre terme de la première suite s'annule.

Il reste encore à chercher si le nombre des V-P peut changer quand les termes de la seconde suite s'annulent. La dérivée de $f_p^2 - k_p f_{p-1} f_{p+1} = T_p$ est

$$(2 - k_p) f_p f_{p+1} - k_p f_{p-1} f_{p+2};$$

pour $T_p = 0$, on a

$$k_p f_{p-1} = \frac{f_p^2}{f_{p+1}},$$

et comme

$$2 - k_p = \frac{1}{k_{p+1}},$$

on peut mettre les dérivées sous la forme

$$\frac{1}{k_{p+1}} \frac{f_p}{f_{p+1}} (f_{p+1}^2 - k_{p+1} f_p f_{p+2}),$$

où la quantité entre parenthèses est le terme suivant T_{p+1} de la suite; on voit ainsi que si x reçoit un accroissement infiniment petit h à partir de la valeur qui annule T_p, T_p reçoit lui-même un accroissement qui a le signe de

$$(4) \qquad \frac{f_p}{f_{p+1}} T_{p+1} h.$$

T_p ne peut changer de signe que si f_{p-1} et f_{p+1} sont de mêmes signes. Si donc on a une V-P, f_p doit avoir un signe opposé à ceux de f_{p+1} et f_{p-1}. La première suite présente alors les signes

$$+ - + \quad \text{ou} \quad - + -,$$

de sorte que $\frac{f_p}{f_{p+1}}$ est négatif et T_p a le signe de

$$-T_{p+1}h.$$

Pour une valeur négative de h, c'est-à-dire avant le passage de T_p par zéro, T_p et T_{p+1} forment une permanence qui, pour h positif, se change en variation; dans ce cas, il se perd une V-P; quand T_{p-1} a même signe que T_{p+1}, il se perd aussi une permanence entre T_{p-1} et T_p, et, dans le cas contraire, il s'en gagne une. *On perd ainsi une* V-P *chaque fois que l'on passe par une racine de $f(x) = 0$; il s'en perd deux toutes les fois qu'un terme de la seconde série passe par zéro quand il est compris entre deux autres de même signe, pendant que le terme correspondant de la première série forme avec le précédent et le suivant une variation.*

117. Nous avons supposé que deux termes consécutifs ne pouvaient pas s'annuler en même temps; s'il en était ainsi, les coefficients de $f(x)$ devraient satisfaire à une équation de condition; alors, en changeant infiniment peu les coefficients, on pourrait ramener ce cas au précédent.

Ce changement n'altère pas les signes des termes des deux suites, pourvu que les valeurs limites de x n'annulent aucun terme. Un changement infiniment petit dans les coefficients ne peut altérer le nombre des racines contenues dans un intervalle donné, si, bien entendu, les valeurs limites ne sont pas racines; la méthode, même dans le cas qui nous occupe, fera connaître une limite supérieure du nombre des racines.

Il reste encore à examiner le cas où $f(x)$, $f'(x)$, ..., $f^{(p-1)}(x)$, $f^{(p)}(x)$ s'annulent : c'est le cas où $p+1$ racines sont égales. On trouve alors, comme à propos du théorème de Budan, que la première suite perd p variations; supposons f_{p+1} positif; la première suite

$$f(x),\quad f'(x),\quad \ldots,\quad f^{(p-1)}(x),\quad f^{(p)}(x),\quad f^{(p+1)}(x)$$

passe de

$$+\quad -\quad +\quad \ldots$$

à

$$+\quad +\quad +\quad \ldots;$$

La seconde série n'a pour $x = h$, dans ses $p+1$ premiers termes, que des permanences. Soit

$$f_r^2 - k_r f_{r-1} f_{r+1}$$

l'un des termes; pour $x = h$, on a

$$f_r = \pm f_{p+1} \frac{h^{p-r+1}}{(p-r+1)!}; \qquad f_{r-1} = \mp f_{p+1} \frac{h^{p-r+2}}{(p-r+2)!};$$
$$f_{r+1} = \mp f_{p+1} \frac{h^{p-r}}{(p-r)!},$$

de sorte que le signe de ce terme sera le même que celui de

$$\frac{1}{[(p-r+1)!]^2} - \frac{k_r}{(p-r+2)!\,(p-r)!}$$

ou de

$$\frac{p-r+2}{p-r+1} - \frac{n-r+1}{n-r}.$$

Cette dernière expression est positive, car $n > p$, et cela quel que soit r. Les deux suites commencent donc pour $x = h$ par p V-P, qui se perdent toutes quand on franchit les p racines; le théorème subsiste donc dans le cas où il y a des racines multiples.

118. En ce qui concerne k_p, nous n'avons utilisé que la relation

$$2 - k_p = \frac{1}{k_{p+1}},$$

et nous avons supposé k_p positif; ces conditions sont remplies si

$$k_p = \frac{m-p+1}{m-p},$$

où $m > n$; quand m croît indéfiniment, cette valeur de k_p se réduit à l'unité.

Exemple :

$$\begin{aligned}
f\ (x) &= x^5 - 3x^4 + 2x^3 - 8x^2 + 3x - 25 = 0,\\
f'\ (x) &= 5x^4 - 12x^3 + 6x^2 - 16x + 3,\\
f''\ (x) &= 20x^3 - 36x^2 + 12x - 16,\\
f'''\ (x) &= 60x^2 - 72x + 12,\\
f^{\text{IV}}(x) &= 120x - 72,\\
f^{\text{V}}\ (x) &= 120.
\end{aligned}$$

Les racines sont comprises entre zéro et 4; pour $x=0$ on a

$$\begin{matrix} -25 & +3 & -16 & +12 & -72 & +120\\ + & - & + & - & + & + \end{matrix}$$

où les signes placés sur la seconde ligne sont ceux des T; pour $x=4$, la première suite ne présente que des permanences, et il n'y a pas besoin de déterminer ceux de la seconde. Pour $x=0$, on a une V-P; pour $x=4$, on n'en a pas; l'équation a donc une racine réelle et quatre racines imaginaires.

119. Dans ce qui précède, on a considéré les V-P perdues pour déterminer le nombre des racines par lesquelles on passe. Sylvester a pris les P-P ou doubles permanences en considération; quand un terme f_p de la première suite, compris entre deux autres de signes contraires, s'annule, les trois termes correspondants de la seconde suite sont positifs, en sorte que une V-P et une P-P changent de place. Si les deux termes qui comprennent celui qui s'annule ont le même signe, les trois termes correspondants de la seconde suite formeront deux variations, de sorte que, dans ce cas, il est encore indifférent de considérer les V-P ou les P-P.

Quand c'est T_p qui change de signe, f_{p-1} et f_{p+1} ont le même signe, de telle sorte que la première suite a deux variations ou deux permanences. Si T_{p-1} et T_{p+1} ont des signes différents, l'ordre seul se trouve modifié : il ne reste donc plus à examiner que le cas où, T_p passant par zéro, T_{p-1} et T_{p+1} sont de mêmes signes.

Dans le cas où la première suite présente deux permanences, (4) montre que T_p, après s'être annulé, prend le signe de T_{p+1}; alors deux P-V se changent en P-P.

Dans le cas où la première suite présente deux variations, (4) montre que, dans la seconde suite, deux permanences se changent en variations; dans ce cas, deux V-P se changent en V-V; on peut donc étendre comme il suit le théorème démontré plus haut :

Quand x croît, en passant par une racine de l'équation donnée, on gagne une P-P; *quand x annule un terme de la seconde suite compris entre deux de même signe, et quand, de plus, les termes correspondants de la première suite présentent deux permanences, on gagne deux* P-P.

120. De cette manière, on a donc deux limites supérieures du nombre des racines réelles, et l'on peut choisir entre celles-ci la moins élevée; c'est ce que l'on voit sur l'exemple traité ci-dessus; pour $x = 0$, on n'a pas de P-P, tandis que pour $x = 4$ on en a cinq; ici le théorème de Sylvester donne cinq racines, tandis que, sous la nouvelle forme que nous avons donnée, il en donne une.

Pour déterminer le nombre des racines réelles d'une équation, on peut faire $x = -\infty$ et $x = +\infty$; il faut alors, dans la seconde suite, déterminer les plus forts exposants de chaque terme; sans s'arrêter aux calculs nécessaires pour cela, on remarquera que, dans T_p, les deux termes avec l'exposant le plus élevé s'évanouissent, de sorte que le terme utile à considérer contient un exposant pair; en laissant de côté un facteur positif, le coefficient de ce terme sera

$$a_1^2 - \frac{2n}{n-1} a_2, \tag{6}$$

l'équation étant

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots = \tag{7}$$

Si donc on avait

$$a_1^2 > \frac{2n}{n-1} a_2,$$

tous les signes de la seconde suite seraient + pour $x = \infty$ comme pour $x = -\infty$; si

$$a_1^2 < \frac{2n}{n-1} a_2,$$

ils seraient —, à l'exception du premier et du dernier, qui seraient +. Dans le premier cas, on gagne n P-P ou l'on perd n V-P, et la méthode ne donne aucun renseignement; dans le second cas, la méthode montre que l'équation a deux racines imaginaires : la méthode ne peut déceler que la présence de deux pareilles racines; pour obtenir un meilleur résultat, il faut partager l'intervalle et, pour chacun des nouveaux intervalles, appliquer le théorème en choisissant la plus petite limite qu'il fournit pour le nombre de racines réelles.

Pour $x = 0$, on tire de (7)

$$f = a_n, \quad f_1 = a_{n-1}, \quad f_2 = 2a_{n-2}, \quad \ldots, \quad f_p = p!\,a_{n-p}, \quad \ldots;$$

il en résulte

$$T_p = (p!)^2 a_{n-p}^2 - \frac{n-p+1}{n-p}(p-1)!(p+1)!\,a_{n-p-1}a_{n-p+1},$$

ou, en écartant le facteur positif $(p!)^2$,

$$T_p = a_{n-p}^2 - \frac{p+1}{p}\,\frac{n-p+1}{n-p}\,a_{n-p-1}a_{n-p+1},$$

formule valable pour tous les termes, sauf pour le premier et le dernier, qui sont positifs.

C'est le seul cas considéré par Newton et pour lequel il a donné son théorème sans démonstration; les deux suites sont alors, en écrivant les termes dans un ordre inverse,

$$\begin{array}{lllll} +, & a_1, & a_2, & a_3, & \ldots \\ +, & a_1^2 - \dfrac{2n}{n-1}a_2, & a_2^2 - \dfrac{3(n-1)}{2(n-2)}a_1a_3, & a_3^2 - \dfrac{4(n-2)}{3(n-3)}a_2a_4, & \ldots. \end{array}$$

Admettons que l'on ait ici q P-P. Pour $x = -\infty$, on n'a pas de P-P; donc *l'équation n'a pas plus de racines négatives que les deux suites n'ont de* P-P (q). *Admettons que les deux suites aient* q_1 V-P ; *pour* $x = +\infty$, *on n'a pas de* V-P : *donc*

l'équation n'a pas plus de racines positives que les deux suites n'ont de V-P (q_1); et l'on peut encore dire que *l'équation a au moins autant de racines imaginaires que la seconde suite a de variations* ($n - q - q_1$).

Newton, en utilisant les P-P pour les valeurs négatives de x et les V-P pour les valeurs positives, obtient une meilleure estimation que Sylvester pour la limite supérieure du nombre des racines réelles. Dans l'exemple traité plus haut, le théorème de Newton montre qu'il n'y a pas plus d'une racine positive, tandis que le théorème de Sylvester, qui n'emploie que les P-P, montre qu'il ne peut en exister plus de cinq. C'est la même limite que donnerait l'application du théorème de Descartes.

Généralisation du théorème de Descartes.

121. Dans ce qui va suivre, nous allons donner une méthode nouvelle qui montre comment, par des considérations toutes différentes, on peut arriver à déterminer une limite du nombre des racines, et qui remplace avec avantage la précédente. Seulement, dans quelques cas particuliers, elle se montre inférieure à celle de Newton, mais elle s'applique avec plus de facilité.

Quand nous avons démontré le théorème de Descartes, nous avons vu que, en introduisant dans l'équation une racine positive, on augmentait au moins d'une unité le nombre des variations. Si la multiplication par $x - \alpha$ introduit plus d'une variation, elle diminue le nombre des permanences, et l'on obtient une détermination plus précise du nombre des racines négatives, le nombre de ces racines n'étant pas augmenté par l'introduction d'une racine positive.

Soit a_p le premier coefficient négatif; l'équation obtenue en multipliant par $x - \alpha$ présentera, à certaines places, les mêmes signes que les termes de l'équation proposée, si l'on écrit les termes les uns au-dessous des autres, et l'on peut se demander si l'on peut choisir α de telle sorte que des permanences se changent en variations.

La multiplication de

(1) $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{p-1} x^{n-p+1} - a_p x^{n-p} \ldots$

par $x - \alpha$ donne

(2) $x^{n+1} + (a_1 - a) x^n + \ldots + (a_{p-1} - \alpha a_{p-2}) x^{n-p+2} - m x^{n-p+1} \ldots,$

où m est positif; maintenant posons

(3) $$\frac{a_r}{a_{r-1}} = k_r,$$

les signes, dans la nouvelle équation, seront ceux de

$$1, \quad k_1 - \alpha, \quad k_2 - \alpha, \quad \ldots, \quad k_{p-1} - \alpha, \quad - \ldots,$$

Soit a_q le premier coefficient positif après $-a_p$; soit $-a_r$ le premier coefficient négatif qui suit, etc., les signes des termes suivants seront ceux de

$$\begin{array}{llllll} -, & \alpha - k_{p+1}, & \alpha - k_{p+2}, & \ldots, & \alpha - k_{q-1}, & \\ +, & k_{q+1} - \alpha, & k_{q+2} - \alpha, & \ldots, & k_{r-1} - \alpha, & \\ -, & \alpha - k_{r+1}, & \alpha - k_{r+2}, & \ldots, & \alpha - k_{s-1}, & \ldots, \\ \ldots, & \ldots\ldots, & \ldots\ldots & \ldots, & \ldots\ldots, & \ldots, \end{array}$$

Dans le cas où les quotients k qui entrent dans chaque groupe sont décroissants, la valeur de α est indifférente; on peut alors déplacer les variations, mais non augmenter leur nombre; dans le cas contraire, il existe une valeur de α comprise entre la plus grande et la plus petite valeur de k d'un groupe qui augmente le nombre des variations; on peut déterminer facilement la valeur de α qui transforme le plus grand nombre possible de permanences en variations; la nouvelle équation peut être traitée comme la première, et ainsi de suite jusqu'à ce que l'on parvienne à une équation où les quotients k sont tous décroissants dans chaque groupe. La limite du nombre des racines positives se déterminera de même façon en changeant x en $-x$.

Exemple :

$$x^8 + x^7 + 4x^6 + 8x^5 - x^4 - 7x^3 - 22x^2 + 152x - 450 = 0,$$

$$1 \quad 4 \quad 2 \qquad 7 \quad \frac{22}{7}$$

les nombres précédents donnent les valeurs des k; si l'on fait $\alpha = 3$, les trois permanences se changent en variations, et l'on n'obtient que des permanences dans

$$-4x^6 - 25x^5 - 4x^4 - x^3 + \ldots$$

$$\frac{25}{4} \quad \frac{4}{25} \quad \frac{1}{4}$$

et l'on a le nouveau groupe de signes

$$-, \quad \alpha - \frac{25}{4}, \quad \alpha - \frac{4}{25}, \quad \alpha - \frac{1}{4}, \quad + \ldots,$$

de sorte que, pour

$$\frac{1}{4} > \alpha > \frac{4}{25},$$

on n'a plus qu'une permanence; l'équation n'a qu'une racine négative.

Le théorème de Newton donne

$$+ \; + \; + \; + \; - \; - \; - \; + \; -$$
$$+ \; - \; + \; + \; + \; + \; + \; + \; +$$

ainsi on a trois P-P. Pour trouver le nombre des racines positives, on change x en $-x$ et l'on a

$$x^8 - x^7 + 4x^6 - 8x^5 - x^4 + 7x^3 - 22x^2 - 152x - 450 = 0;$$

dans les dernières permanences, les quotients k vont en diminuant, et la multiplication ne peut faire disparaître de permanences. L'équation a donc une ou trois racines positives, ce que nous apprend aussi la méthode de Newton.

CHAPITRE II.

CALCUL DES RACINES DES ÉQUATIONS NUMÉRIQUES.

Calcul des racines commensurables.

122. Une équation à coefficients fractionnaires peut toujours, comme on l'a vu (42), être remplacée par une autre à coefficients entiers, le premier terme ayant pour coefficient l'unité. Dans la suite nous supposerons toujours qu'il en est ainsi.

Une équation à coefficients entiers et dont le premier terme a pour coefficients l'unité ne saurait avoir de racines fractionnaires.

Soit l'équation

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0. \tag{1}$$

Si la fraction irréductible $\frac{p}{q}$ pouvait être racine de cette équation, on aurait

$$\frac{p^n}{q^n} = -\left(a_1 \frac{p^{n-1}}{q^{n-1}} + a_2 \frac{p^{n-2}}{q^{n-2}} + \ldots + a_n\right),$$

ou

$$\frac{p^n}{q} = -\left(a_1 p^{n-1} + a_2 p^{n-2} q + \ldots + a_n q^{n-1}\right),$$

ce qui est impossible, vu que le premier membre est une fraction irréductible, tandis que le second membre est entier.

123. Si l'on veut alors calculer les racines rationnelles d'une équation, on peut d'abord la mettre sous une forme telle qu'elle n'ait plus que des coefficients entiers; le premier étant égal à 1, elle n'a plus en fait de racines rationnelles que des racines entières, et nous allons montrer comment on peut déterminer ces dernières.

Soit (1) l'équation donnée et t une racine entière, on a

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots + a_{n-2} t^2 + a_{n-1} t + a_n = 0;$$

il faut remarquer tout d'abord que t est un diviseur de a_n; on essayera donc les diviseurs de a_n, et si aucun d'eux n'est racine, l'équation proposée n'a pas de racine entière.

Pour essayer le nombre t, on divisera l'équation précédente par t et, si l'on fait $a_n = tq_{n-1}$, on aura

$$t^{n-1} + a_1 t^{n-2} + a_2 t^{n-3} + \ldots + a_{n-1} + q_{n-1} = 0,$$

d'où il résulte que $a_{n-1} + q_{n-1}$ doit être divisible par t; appelons q_{n-2} le quotient, on voit de même que $a_{n-2} + q_{n-2}$ doit être divisible par t, et finalement on a

$$1 + q_0 = 0.$$

Dès que dans le courant des opérations un quotient q devient fractionnaire, le nombre t essayé ne peut être racine. Au contraire, si tous les coefficients sont entiers et si l'on termine par $q_0 = -1$, le nombre essayé est racine et le premier membre de l'équation, débarrassé du facteur linéaire correspondant à cette racine, est

$$x^{n-1} - q_1 x^{n-2} - q_2 x^{n-3} - \ldots - q_{n-1},$$

car, en multipliant le polynome par $x - t$, on trouve

$$x^n - (q_1 + t) x^{n-1} + \ldots + (tq_{p-1} - q_p) x^{n-p} + \ldots + tq_{n-1}$$

et comme

$$a_p + q_p = tq_{p-1},$$

ou

$$tq_{p-1} - q_p = a_p,$$

on retrouve le premier membre de (1). L'exemple suivant rendra évidente la marche des calculs.

Exemple :

$$x^5 - 47x^4 + 423x^3 - 140x^2 + 1213x + 420 = 0.$$

Essayons, par exemple, le nombre 3, on aura

$$\begin{array}{ccc} \ldots - 140x^2 & + 1213x & + 420 \\ 451 & 140 & \\ \hline 311 & 1353 & \end{array}$$

3 ne divise pas 311 et ne peut être racine; essayons 12, on a

$$\begin{array}{cccccc} 1 & -47 & 423 & -140 & 1213 & 420 \\ -1 & 35 & -3 & 104 & 35 & \\ \hline 0 & -12 & 420 & -36 & 1248 & \end{array}$$

12 est racine et l'équation divisée par $x - 12$ donne

$$x^4 - 35x^3 + 3x^2 - 104x - 35 = 0;$$

en essayant $x = 35$, on a

$$\begin{array}{ccccc} 1 & -35 & 3 & -104 & -35 \\ -1 & 0 & -3 & -1 & \\ \hline & -35 & 0 & -105 & \end{array}$$

et l'on arrive à l'équation

$$x^3 + 3x + 1 = 0$$

qui n'a plus de racines rationnelles.

Pour diminuer le nombre des essais infructueux, il faut déterminer les limites des racines; on diminue ainsi le nombre des facteurs de a_n à essayer en éliminant ceux qui sont compris en dehors des limites. Il faut ensuite observer que, si $f(x)$ est divisible par $x - t$, les nombres

$$\frac{f(1)}{t-1}, \quad \frac{f(-1)}{t+1}, \quad \frac{f(2)}{t-2}, \quad \frac{f(-2)}{t+2}, \quad \ldots$$

doivent être entiers; les nombres les plus petits -1, $+1$,

substitués dans l'équation, donnent $f(1)$, $f(-1)$ et, dans l'exemple précédent, on a

$$f(-1) = -1404; \qquad f(1) = 1870.$$

Il n'est donc pas nécessaire d'essayer le nombre 10, car 1404 n'est pas divisible par 11; il faut essayer, au contraire, -10 parce que 1404 est divisible par 9 et 1870 par 11; on a

$$f(2) = 4950$$

qui n'est pas divisible par 12. On voit alors que -10 n'est pas racine.

Interpolation.

124. Lorsque l'on a séparé les racines d'une équation, il est nécessaire de rapprocher, autant que possible, les limites qui comprennent cette racine, avant d'appliquer les méthodes d'approximation. On arrive à ce résultat en substituant des valeurs intermédiaires dans $f(x)$, et l'on peut continuer ainsi jusqu'à ce que l'on ait repéré les racines entre des limites aussi rapprochées que l'on veut.

Bien que cette méthode soit théoriquement assez simple, elle ne laisse pas que d'être très pénible en pratique, et l'on suit une autre voie qui permet d'arriver plus facilement au but.

125. *Différences d'une fonction.* — Soit

$$u_0, \quad u_1, \quad u_2, \quad \ldots$$

une suite de quantités déterminées d'une manière quelconque; si l'on pose

$$u_{n+1} - u_n = \Delta u_n, \tag{1}$$

Δu_n est ce que l'on appelle la première différence de u_n; on construit d'une manière analogue la seconde, la troisième différence, etc. Ainsi

$$\left\{\begin{array}{l} \Delta u_{n+1} - \Delta u_n = \Delta^2 u_n, \\ \Delta^2 u_{n+1} - \Delta^2 u_n = \Delta^3 u_n, \text{ etc.}; \end{array}\right. \tag{2}$$

on en déduit

$$\begin{aligned}\Delta^2 u_n &= \Delta u_{n+1} - \Delta u_n \\ &= u_{n+2} - u_{n+1} - u_{n+1} + u_n \\ &= u_{n+2} - 2u_{n+1} + u_n,\end{aligned}$$

$$\begin{aligned}\Delta^3 u_n &= \Delta(u_{n+2} - 2u_{n+1} + u_n) \\ &= u_{n+3} - 2u_{n+2} + u_{n+1} - u_{n+2} + 2u_{n+1} - u_n \\ &= u_{n+3} - 3u_{n+2} + 3u_{n+1} - u_n;\end{aligned}$$

comme on voit, les coefficients sont ceux des puissances de $a - b$ et l'on a en général

$$(3) \qquad \Delta^p u_n = u_{n+p} - \frac{p}{1} u_{n+p-1} + \frac{p(p-1)}{1.2} u_{n+p-2} + \ldots + (-1)^p u_n,$$

et l'on voit que les différences peuvent s'exprimer en fonction des termes de la suite u_0, u_1, ... Réciproquement, les termes de la suite peuvent s'exprimer à l'aide des différences. On a, en effet,

$$u_1 = u_0 + \Delta u_0;$$

d'où

$$\Delta u_1 = \Delta u_0 + \Delta^2 u_0;$$

mais

$$u_2 = u_1 + \Delta u_1,$$

donc

$$u_2 = u_0 + 2\Delta u_0 + \Delta^2 u_0.$$

De même

$$\begin{aligned}u_3 &= u_2 + \Delta u_2 \\ &= u_0 + 2\Delta u_0 + \Delta^2 u_0 + \Delta u_0 + 2\Delta^2 u_0 + \Delta^3 u_0 \\ &= u_0 + 3\Delta u_0 + \Delta^2 3 u_0 + \Delta^3 u_0,\end{aligned}$$

et l'on voit que les coefficients sont ceux des puissances de $a + b$. On a ainsi, en général,

$$(4) \qquad u_p = u_0 + \frac{p}{1} \Delta u_0 + \frac{p(p-1)}{1.2} \Delta^2 u_0 + \ldots + \Delta^p u_0.$$

126. *Différences des fonctions entières.* — Soit

$$(5) \qquad u = f(x) = a_0 x^n + a_1 x^{n-1} + \ldots$$

une fonction entière de x, dans laquelle on donnera à x successivement les valeurs

$$x_0; \quad x_0+h; \quad x_0+2h; \quad \ldots; \quad x_0+nh;$$

soient

$$u_0, \quad u_1, \quad u_2, \quad \ldots, \quad u_n$$

les valeurs correspondantes de u.

On a alors

$$(6) \qquad \Delta u = f(x+h) - f(x) = na_0 x^{n-1} h + \ldots$$

et il en résulte que Δu est de degré inférieur d'une unité au degré de u; $\Delta^2 u$ est de degré inférieur de deux unités et a pour premier terme $n(n-1)a_0 x^{n-2} h^2$, etc.; il en résulte que *lorsqu'une fonction est de degré n, sa $n^{\text{ième}}$ différence est constante* et

$$\Delta^n u = n!\, a_0 h^n.$$

Les différences d'ordre supérieur sont nulles. *Une suite dont les différences d'ordre n sont constantes est une suite différentielle d'ordre n.*

Exemple :

$$f(x) = x^4, \qquad h = 1; \qquad x_0 = 1$$

$$\begin{array}{ccccccccc}
u_0 & & u_1 & & u_2 & & u_3 & & u_4 \\
1 & & 16 & & 81 & & 256 & & 625 \quad \ldots \\
& \Delta u_0 & & \Delta u_1 & & \Delta u_2 & & \Delta u_3 & \ldots \\
& 15 & & 65 & & 175 & & 369 & \ldots \\
& & \Delta^2 u_0 & & \Delta^2 u_1 & & \Delta^2 u_2 & & \ldots \\
& & 50 & & 110 & & 194 & & \ldots \\
& & & \Delta^3 u_0 & & \Delta^3 u_1 & & & \ldots \\
& & & 60 & & 84 & & & \ldots \\
& & & & \Delta^4 u_0 & & & & \ldots \\
& & & & 24 & & & & \ldots.
\end{array}$$

Les formules (4) et (3) donnent

$$u_5 = 1 + 5.15 + 10.50 + 10.60 + 5.24 = 1296 = 6^4,$$
$$\Delta^4 u_0 = 1 - 4.16 + 6.81 - 4.256 + 625 = 24.$$

127. *Substitution de valeurs équidistantes de x dans $f(x)$.* — Si l'on veut calculer $f(x)$ pour des valeurs équidistantes de x, on peut le faire pour n valeurs équidistantes de x et obtenir les autres valeurs de $f(x)$ au moyen de simples additions.

Supposons, par exemple, que la fonction donnée soit

$$u = x^3 - 5x + 6,$$

et que l'on désire en obtenir les valeurs pour $x = 1, 2, 3, \ldots$; alors si $x_0 = 1$, pour

$$x = 1, \qquad x = 2, \qquad x = 3,$$

u	Δu	$\Delta^2 u$	$\Delta^3 u$
2			
	2		
4		12	6
	14		
18			

Comme l'on sait, la dernière différence est 6. Pour $\Delta^2 u$, le calcul peut se faire en observant que les différences de deux différences secondes est égale à 6; il suffira d'avoir une seule différence première pour avoir toutes les autres quand on connaîtra les différences secondes et, enfin, on aura toutes les valeurs de u dès que l'on aura l'une d'elles; il suffira donc d'avoir calculé trois valeurs de u et d'en déduire directement deux valeurs de Δu, puis une de $\Delta^2 u$. On trouve ainsi, pour $\Delta^2 u$,

$$6, \quad 12, \quad 18, \quad \ldots,$$

puis, pour Δu,

$$-4, \quad 2, \quad 14, \quad 32, \quad \ldots,$$

puis, pour u,

$$6, \quad 2, \quad 4, \quad 18, \quad 50, \quad \ldots;$$

ainsi l'on trouve

$$f(0) = 6, \qquad f(4) = 50.$$

128. *Calcul de $f(x)$ au moyen de ses valeurs pour $n+1$ valeurs équidistantes de x.* — Si l'on écrit la formule (4)

sous la forme

$$(7)\quad \left\{ \begin{aligned} u_p = u_0 + \frac{p}{1}\Delta u_0 + \frac{p(p-1)}{1.2}\Delta^2 u_0 + \ldots \\ + \frac{p(p-1)\ldots(p-n+1)}{1.2.3\ldots n}\Delta^n u_0; \end{aligned} \right.$$

et si l'on y fait

$$p = \frac{x - x_0}{h},$$

puis si l'on y suppose u_0, Δu_0, $\Delta^2 u_0$, ... remplacés par leurs valeurs déduites de $u = f(x)$, on a

$$(8)\quad \left\{ \begin{aligned} u_{\frac{x-x_0}{h}} = u_0 + \frac{x-x_0}{1}\frac{\Delta u_0}{h} + \frac{(x-x_0)(x-x_0-h)}{1.2}\frac{\Delta^2 u_0}{h^2} + \ldots \\ + \frac{(x-x_0)(x-x_0-h)\ldots[x-x_0-(n-1)h]}{1.2.3\ldots n}\frac{\Delta^n u_0}{h^n}. \end{aligned} \right.$$

Comme cette formule a lieu pour toutes les valeurs entières de p, elle aura lieu aussi pour

$$x = x_0, \qquad x = x_0 + h, \qquad x = x_0 + 2h, \qquad \ldots, \qquad x = x_0 + nh.$$

Si l'on désigne le second membre par $F(x)$, on aura donc

$$f(x) = F(x)$$

pour $n+1$ valeurs de x; comme cette équation est au plus de degré n, c'est une identité; on a donc exprimé $f(x)$ au moyen de ses valeurs pour $n+1$ valeurs équidistantes de x, et cela sous une forme qui est souvent utile.

Exemple. — Trouver une fonction du troisième degré prenant pour $x=1$, $x=2$, $x=3$, $x=4$ les valeurs 5, 11, 13 et 21. On a

$$\begin{array}{ccccccc} 5 & & 11 & & 13 & & 21 \\ & 6 & & 2 & & 8 & \\ & & -4 & & +6 & & \\ & & & 10 & & & \end{array}$$

ainsi

$$u_0 = 5, \qquad \Delta u_0 = 6, \qquad \Delta^2 u_0 = -4, \qquad \Delta^3 u_0 = 10, \qquad h = 1,$$

donc

$$f(x) = 5 + 6(x-1) - 2(x-1)(x-2) + \frac{5}{3}(x-1)(x-2)(x-3).$$

129. *Interpolation.* — A l'aide du théorème précédent, on peut résoudre la question que nous nous étions proposée, à savoir de calculer des valeurs d'une fonction, pour des valeurs de x comprises entre celles pour lesquelles le calcul a déjà été fait. Ordinairement, on partage h en parties égales; on pose, par exemple,

$$h = qh_1;$$

on a alors les valeurs de la fonction pour $x = x_0 + mh_1$ au moyen de la formule (8)

$$v_m = f(x_0 + mh_1) = u_0 + A_1 \Delta u_0 + A_2 \Delta^2 u_0 + \ldots + A_n \Delta^n u_0$$

où

$$(9) \qquad A_k = \frac{m(m-q)(m-2q)\ldots[m-(k-1)q]}{1.2.3\ldots kq^k}.$$

Si l'on pose, par exemple,

$$h = 1, \qquad h_1 = \frac{1}{10},$$

on a

$$(10) \qquad A_k = \frac{m(m-10)(m-20)\ldots[m-10(k-1)]}{1.2.3\ldots k10^k}.$$

Pour calculer $f(x_0 + mh_1)$, on ne substitue pas les valeurs de m dans A_k; on se borne à calculer les différences de la fonction correspondant au nouvel intervalle et, si on les désigne par la caractéristique δ, on a

$$\begin{aligned}
v_0 &= u_0,\\
\delta v_0 &= \delta A_1 \Delta u_0 + \delta A_2 \Delta^2 u_0 + \delta A_3 \Delta^3 u_0 + \ldots,\\
\delta^2 v_0 &= \qquad\qquad \delta^2 A_2 \Delta^2 u_0 + \delta^2 A_3 \Delta^3 u_0 + \ldots,\\
\delta^3 v_0 &= \qquad\qquad\qquad\qquad \delta^3 A_3 \Delta^3 u_0 + \ldots,
\end{aligned}$$

car

$$\delta u_0 = 0, \qquad \delta^2 A_1 = 0, \qquad \delta^3 A_2 = 0, \qquad \ldots,$$

parce que u_0, A_1, A_2, ... sont de degrés 0, 1, 2, ... en m res-

pectivement; on a, pour $q = 10$, $m = 0$,

$$A_1 = \frac{m}{10}, \qquad \delta A_1 = 0,1,$$

$$A_2 = \frac{m(m-10)}{1.2.10^2}, \qquad \delta A_2 = -0,045, \qquad \delta^2 A_2 = 0,01,$$

$$A_3 = \frac{m(m-10)(m-20)}{1.2.3.10^3}, \qquad \delta A_3 = 0,0285, \qquad \delta^2 A_3 = -0,009,$$
$$\delta^3 A_3 = \quad 0,001.$$

Dans la fonction considérée plus haut, on avait

$$u_0 = 5, \qquad \Delta u_0 = 6, \qquad \Delta^2 u_0 = -4, \qquad \Delta^3 u_0 = 10;$$

alors

$$\delta v_0 = 6.0,1 + 4.0,045 + 10.0,0285 = 1,065,$$
$$\delta^2 v_0 = -4.0,01 - 10.0,009 = -0,13,$$
$$\delta^3 v_0 = 10.0,001 = 0,01.$$

Les valeurs de la fonction pour

$$x = 1,1, \qquad x = 1,2, \qquad \ldots, \qquad x = 1,9$$

sont fournies par le Tableau :

x.	u.	δu.	$\delta^2 u$.	$\delta^3 u$.
1,0.........	5,000	1,065	−0,13	0,01
1,1.........	6,065	0,935	−0,12	0,01
1,2.........	7,000	0,815	−0,11	0,01
1,3.........	7,815	0,705	−0,10	0,01
1,4.........	8,520	0,605	−0,09	0,01
1,5.........	9,125	0,515	−0,08	0,01
1,6.........	9,640	0,435	−0,07	0,01
1,7.........	10,075	0,365	−0,06	0,01
1,8.........	10,440	0,305	−0,05	
1,9.........	10,745	0,255		
2,0.........	11,000			

Si l'on prolonge ce Tableau par le haut, on trouve que la fonction s'annule pour une valeur de x comprise entre $x = 0,6$ et $x = 0,7$.

Méthode d'approximation de Newton.

130. Supposons qu'une racine de $f(x)=0$ soit séparée par deux nombres voisins a et b où $a<b$. Si l'on pose $x=a$, on a une erreur x_1 déterminée par l'équation

$$f(a+x_1)=0 \qquad \text{ou} \qquad 0=f(a)+f'(a)x_1+\frac{1}{2}f''(a)x_1^2+\ldots;$$

comme x_1 est très petit, les termes en x_1^2, x_1^3, ... sont très petits en comparaison de ceux qui contiennent x_1. Newton les néglige et pose

$$0=f(a)+f'(a)x_1, \qquad \text{d'où} \qquad x_1=-\frac{f(a)}{f'(a)};$$

d'où

$$x=a-\frac{f(a)}{f'(a)}. \tag{1}$$

On obtient ainsi une valeur approchée qui, en général, sera plus satisfaisante que la première ; de celle-ci on en déduira une autre par le même procédé, et ainsi de suite.

Exemple :

$$x^3-2x-5=0;$$

une racine est comprise entre 2 et 2,1, on a

$$f(x)=x^3-2x-5,$$
$$f'(x)=3x^2-2;$$

si l'on fait $a=2$, on a

$$x=2-\frac{-1}{10}=2,1;$$

on a

$$f(2,1)=0,061; \qquad f'(2,1)=11,23,$$

d'où

$$x=2,1-0,0054=2,0946,$$

et de là on déduit encore

$$x = 2,0946 - \frac{f(2,0946)}{f'(2,0946)} = 2,0946 - 0,000048517$$
$$= 2,094551483.$$

131. *Défaut de la méthode.* — La méthode de Newton est d'une application assez simple, mais elle ne peut pas toujours être employée avec certitude, parce qu'il peut arriver que l'erreur, au lieu de s'atténuer, aille en grossissant. On s'en rend compte au moyen d'une représentation géométrique; on doit déterminer l'intersection de la courbe $y = f(x)$ avec l'axe des x. On a trouvé un point dans le voisinage du point

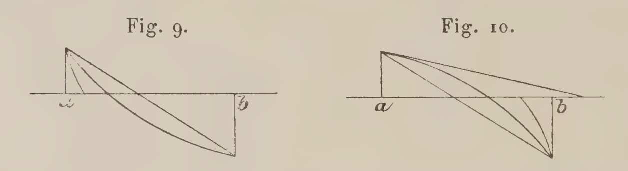


Fig. 9. Fig. 10.

d'intersection, qui a pour abscisse a; la méthode de Newton revient à remplacer la courbe par sa tangente au point qui a pour abscisse a; cette tangente a, en effet, pour équation

$$y - f(a) = f'(a)(x - a),$$

et son intersection avec l'axe des x s'obtient en faisant $y = 0$; d'où

$$x = a - \frac{f(a)}{f'(a)},$$

ce qui est la formule de Newton; on voit que le point où la tangente coupe l'axe des x peut être plus éloigné du point cherché que le point d'où l'on est parti. Pour cette raison (Fourier, Housel, etc.), on a cherché à perfectionner la méthode de manière à approcher constamment de la racine cherchée. Pour arriver au but, il faut connaître une valeur approchée par excès et une valeur approchée par défaut. Ce qui suit va résulter des explications que nous venons de donner.

132. Nous supposerons l'équation débarrassée de ses racines multiples. Nous supposerons, en outre, que $f'(x)$ et $f''(x)$ ne soient pas nuls en même temps. On peut alors supposer que les limites de la racine cherchée soient assez rapprochées pour que, entre ces limites, $f'(x)$ et $f''(x)$ ne changent pas de signe. L'ordonnée de la courbe $y=f(x)$ est alors, entre ces limites, toujours croissante ou toujours décroissante, et sa concavité est toujours tournée du même côté; comme $f(x)$ change de signe dans l'intervalle, $f(x)$ et $f''(x)$ ont le même signe à l'une des limites; si l'on part de cette limite, la méthode de Newton fournira une valeur plus approchée, ainsi que l'on peut s'en assurer à l'inspection des quatre figures ci-dessous :

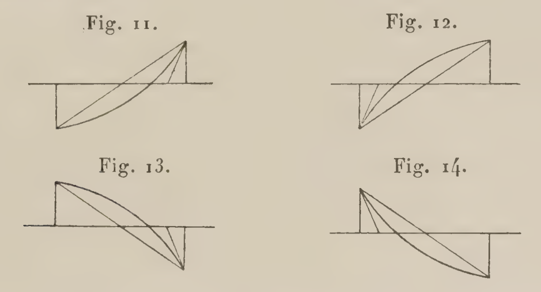


Fig. 11. Fig. 12. Fig. 13. Fig. 14.

Dans la première et dans la dernière figure, $f''(x)$ est positif, et l'on part de la limite pour laquelle $f(x)$ est positif; dans les deux autres, $f''(x)$ est négatif et l'on part de la limite pour laquelle $f(x)$ est négatif. Si l'on mène une sécante passant par les points correspondants aux deux limites, cette sécante coupe l'axe des x en un point qui, avec le point où la tangente rencontre le même axe, fournit deux limites plus rapprochées entre lesquelles la racine se trouve comprise; la sécante a pour équation

$$y-f(a)=\frac{f(b)-f(a)}{b-a}(x-a),$$

et elle donne

$$x=a-f(a)\frac{b-a}{f(b)-f(a)}=a-\frac{f(a)}{f'(a)+m}$$

ou

$$f(b) = f(a) + f'(a)\frac{b-a}{1} + f''(a)\frac{(b-a)^2}{1.2} + \ldots,$$

$$m = \frac{1}{2}f''(a)(b-a) + \frac{1}{2.3}f'''(a)(b-a)^2 + \ldots.$$

Si donc a et b sont deux limites telles que $f(a)$ et $f''(a)$ soient de même signe

$$a_1 = a - \frac{f(a)}{f'(a)}$$

et

$$b_1 = a - \frac{f(a)}{f'(a) + m}$$

sont deux nouvelles limites plus approchées.

Exemple. — Nous avons considéré l'équation

$$x^3 - 2x - 5 = 0,$$

où

$$f(x) = x^3 - 2x - 5; \qquad f'(x) = 3x^2 - 2; \qquad f''(x) = 6x.$$

Une racine est séparée par les limites 2 et 2,1 ; on a

$$f(2) = -1, \qquad f(2,1) = 0,061$$

et $f''(2,1)$ est positif.

$$a_1 = 2,1 - 0,0054 = 2,0946,$$

$$b_1 = 2,1 - \frac{0,061}{10,61} = 2,0942.$$

Si l'on part de ces nouvelles limites, on trouve

$$a_2 = 2,094551483,$$
$$b_2 = 2,0946 - 0,000048528 = 2,094551472.$$

Méthode de Lagrange.

133. Lorsqu'une racine se trouve séparée par deux entiers consécutifs a et $a+1$, on peut poser

$$x = a + \frac{1}{x_1}$$

et former l'équation en x_1; si la racine cherchée était négative, on changerait x en $-x$.

Si l'équation proposée n'a qu'une racine entre a et $a+1$, la transformée n'a qu'une racine supérieure à 1; celle-ci pourra être séparée par deux entiers b et $b+1$, et l'on posera

$$x_1 = b + \frac{1}{x_2}.$$

En poursuivant ainsi les calculs, on obtient le développement de la racine en fraction continue

$$x = a + \cfrac{1}{b + \cfrac{1}{c_{\ddots}}}$$

Si l'équation proposée avait plusieurs racines entre a et $a+1$, la transformée aurait plusieurs racines supérieures à 1; chacune d'elles donnerait lieu à un calcul analogue.

Exemple :

$$f(x) = x^3 - 2x - 5 = 0,$$

on pose

$$x = 2 + \frac{1}{x_1};$$

on a

$$f(x) = f(2) + f'(2)\frac{1}{x_1} + \frac{1}{2}f''(2)\frac{1}{x_1^2} + \frac{1}{x_1^3}$$

$$= -1 + 10\frac{1}{x_1} + 6\frac{1}{x_1^2} + \frac{1}{x_1^3},$$

et la transformée

$$f_1(x_1) = x_1^3 - 10x_1^2 - 6x_1 - 1 = 0;$$

la racine positive de cette équation est comprise entre 10 et 11; on pose

$$x_1 = 10 + \frac{1}{x_2}.$$

On a

$$f_1(x) = x^3 - 10x^2 - 6x - 1, \qquad f_1(10) = -61,$$

$$f_1'(x) = 3x^2 - 20x - 6, \qquad f_1'(10) = +94,$$

$$\frac{1}{1.2}f_1''(x) = 32x - 10, \qquad \frac{1}{2}f_1''(10) = +20,$$

et la transformée est

$$-61x_2^3+94x_2^2+20x_2+1=0,$$

dont la racine positive est comprise entre 1 et 2.

La racine cherchée est comprise entre

$$2+\cfrac{1}{10+\cfrac{1}{1}} \quad \text{et} \quad 2+\cfrac{1}{10+\cfrac{1}{2}},$$

ou entre

$$\frac{23}{11} \quad \text{et} \quad \frac{44}{21}.$$

134. Cette méthode ne conduit que péniblement à une approximation convenable. Lagrange a montré comment on pouvait simplifier la dernière partie du calcul; mais, comme les calculs sont encore compliqués, malgré ce perfectionnement, la méthode n'est pas avantageuse et, pour cette raison, nous ne l'exposerons pas. Au contraire, nous montrerons que cette méthode peut être remplacée par une autre plus avantageuse en profitant de la forme particulière de l'équation transformée.

Considérons l'équation trouvée plus haut

$$f_1(x_1)=x_1^3-10x_1^2-6x_1-1=0.$$

Si l'on développe en série récurrente une fraction dont le dénominateur est $f_1(x)$, cette série passera de l'état de convergence à l'état de divergence quand x_1 passera par la racine cherchée et rendra la fraction infinie; développons alors $\frac{x^3}{f_1(x)}$, nous aurons

$$\frac{x^3}{f_1(x)}=1+\frac{a_1}{x}+\frac{a_2}{x^2}+\ldots,$$

où les coefficients sont liés par la relation

$$a_n=10a_{n-1}+6a_{n-2}+a_{n-3};$$

on trouvera successivement, pour ces coefficients, les valeurs

$$1,\quad 10,\quad 106,\quad 1121,\quad 11856,\quad 125392,\quad 1326177,\quad \ldots.$$

En vertu d'un théorème de Cauchy, lorsque la série de convergente devient divergente, le rapport d'un terme au précédent passe par la valeur 1; ce rapport est

$$\frac{a_{n+1}}{a_n}\frac{1}{x_1},$$

de sorte que $\frac{a_n}{a_{n+1}}$ tend vers $\frac{1}{x_1}$; en faisant usage des deux derniers coefficients calculés, on trouve

$$x = 2 + \frac{1}{x_1} = 2,09\,45\,51\,4815.$$

Si l'on calcule encore un coefficient, celui-ci et le précédent fourniront une valeur de x qui a, avec celle que nous venons de trouver, dix décimales communes.

135. Cette méthode revient, au fond, à celle que Daniel Bernoulli a fait connaître; voici en quoi elle consiste :

Calculons les fonctions symétriques des racines

$$s_m = x_1^m + x_2^m + x_3^m + \ldots,$$
$$s_{m+1} = x_1^{m+1} + x_2^{m+1} + x_3^{m+1} + \ldots,$$

Si x_1 est la plus grande racine, pour une grande valeur de m, s_m et s_{m+1} pourront être remplacées par leurs premiers termes et l'on aura

$$x_1 = \frac{s_{m+1}}{s_m}.$$

En faisant usage de s_{-m} et $s_{-(m+1)}$, on peut de même trouver la plus petite racine.

Si l'on observe alors que

$$\frac{xf'(x)}{f(x)} = n + \frac{s_1}{x} + \frac{s_2}{x^2} + \ldots,$$

on voit que la méthode exposée plus haut coïncide avec celle de Bernoulli quand on prend $xf'(x)$ pour numérateur.

Cette remarque montre dans quel cas il sera avantageux d'employer la méthode. Pour que tous les termes que l'on

néglige soient petits par rapport à x_1^m, il faut qu'il n'existe pas de racine ayant une valeur absolue voisine de celle de x_1, ni de racine imaginaire dont le module diffère peu de celui de x_1. Si deux racines imaginaires ont un module maximum, le rapport de deux sommes consécutives ne tendra vers aucune limite; si, par exemple, ces racines sont

$$r(\cos\theta \pm i\sin\theta),$$

on aura

$$s_m = 2r^m \cos m\theta + \ldots,$$
$$s_{m+1} = 2r^{m+1}\cos(m+1)\theta + \ldots,$$

et, en négligeant les termes d'ordre inférieur,

$$\frac{s_{m+1}}{s_m} = r\frac{\cos(m+1)\theta}{\cos m\theta}.$$

m croissant indéfiniment, cette expression n'a pas de limite. L'emploi des séries entières conduit aux mêmes conclusions. Pour que l'on puisse appliquer la méthode avec succès, il faut que l'on puisse mettre l'équation sous une forme telle que les termes de l'échelle de relation aient le même signe et décroissent assez rapidement; la méthode pourra donc s'appliquer concurremment avec la méthode de Lagrange qui, en général, conduit rapidement à une équation transformée jouissant de la propriété requise.

136. Nous traiterons encore un exemple. L'équation

$$x^3 - 7x + 7 = 0$$

a deux racines comprises entre 1 et 2; si l'on pose

$$x = 1 + \frac{1}{x_1},$$

on obtient la transformée

$$x_1^3 - 4x_1^2 + 3x_1 + 1 = 0,$$

qui a une racine entre 1 et 2 et une autre entre 2 et 3; on devra traiter chacune à son tour; en considérant la seconde

on posera

$$x_1 = 2 + \frac{1}{x_2},$$

d'où l'on déduit

$$x_2^3 + x_2^2 - 2x_2 - 1 = 0,$$

qui a une racine positive entre 1 et 2; on posera

$$x_2 = 1 + \frac{1}{x_3},$$

et l'on aura

$$x_3^3 - 3x_3^2 - 4x_3 - 1 = 0;$$

la racine positive de cette équation est comprise entre 4 et 5. Posons enfin

$$x_3 = 4 + \frac{1}{x_4},$$

on obtient la transformée

$$x_4^3 - 20x_4^2 - 9x_4 - 1 = 0;$$

l'échelle de relation est

$$20, \quad 9, \quad 1,$$

et, à l'aide de ces nombres, on forme les coefficients

$$1, \quad 20, \quad 409, \quad 8361, \quad 170921, \quad 349078.$$

Si l'on pose

$$x_4 = \frac{3494078}{170921},$$

on a

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{x_4}}}} \cdot \cdot \cdot,$$

où

$$x = \frac{19.3494078 + 4.170921}{14.3494078 + 3.170921} = 1.3568958.$$

137. Après la méthode de Bernoulli, il convient de mentionner celle de Gräffe. Elle consiste à poser $x = \sqrt{y}$ et à faire évanouir le radical; on obtient alors une équation dont les

racines sont les carrés des racines de la proposée; si l'on continue de la sorte en calculant les coefficients par logarithmes, si l'on finit par trouver une transformée dans laquelle les logarithmes des coefficients vont en doublant : c'est un signe que les racines sont négligeables vis-à-vis de la plus grande. Supposons, par exemple, que l'on ait élevé les racines à la trente-deuxième puissance et que l'on ait obtenu l'équation

$$z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots = 0.$$

Si l'on pose

$$x_1^{32} = -a_1,$$
$$x_1^{32} x_2^{32} = a_2,$$
$$x_1^{32} x_2^{32} x_3^{32} = -a_3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

en négligeant les termes d'ordre inférieur, on trouve les racines quand elles sont réelles, mais la présence des racines imaginaires complique la question comme dans la méthode de Bernoulli; aussi n'entrons-nous pas dans plus de détails.

Méthode de Horner.

138. La méthode de Horner s'appuie sur ce fait que, étant donnée une équation, on peut en déduire une autre dont les racines sont égales à celles de la proposée, diminuées d'une même quantité; la méthode tire son importance de la manière même dont se fait la transformation, qui est assez simple.

Soit

$$f(x) = 0$$

l'équation donnée; pour diminuer les racines de α, on prend pour nouvelle inconnue $x - \alpha$ et l'on pose

$$f(x) = f(\alpha + x - \alpha) = f(\alpha) + f'(\alpha)(x - \alpha) + \frac{f''(\alpha)}{1.2}(x - \alpha)^2 + \ldots + (x - \alpha)^n = 0.$$

On voit que $f(\alpha)$ est le reste de la division de $f(x)$ par $x - \alpha$, que $f'(\alpha)$ est le reste obtenu en divisant le quotient

par $x-\alpha$, etc.; par des divisions successives par $x-\alpha$, on obtient les termes successifs de l'équation transformée.

Pour effectuer la division par $x-\alpha$, on peut faire usage de la méthode employée pour développer une fraction en série, l'échelle de relation est α; si le dividende est

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$

et le quotient

$$b_0 x^{n-1} + b_1 x^{n-2} + b_2 x^{n-3} + \ldots + b_{n-1} + \frac{b_n}{x-\alpha},$$

on a

$$b_0 = a_0, \quad b_1 = a_1 + \alpha b_0, \quad b_2 = a_2 + \alpha b_1, \quad \ldots, \quad b_p = a_p + \alpha b_{p-1} \quad \ldots.$$

On a l'habitude de disposer les calculs comme on va l'indiquer à propos des racines de l'équation

$$3x^5 - x^3 + 4x^2 + 5x - 8 = 0,$$

en diminuant les racines de deux unités; on a, en n'écrivant que les coefficients,

3	0	—1	+4	+5	—8
3	6	11	26	57	106
3	12	35	96	249	
3	18	71	238		
3	24	119			
3	30				

l'équation transformée est ainsi

$$3x^5 + 30x^4 + 119x^3 + 238x^2 + 249x + 106 = 0.$$

La multiplication par $2(\alpha)$ et l'addition ont été menées de front; si l'on avait affaire à des nombres composés d'un plus grand nombre de chiffres et qu'il fût impossible de faire les opérations de tête, il serait bon d'écrire le produit αb_p au-dessous de a_{p+1} et d'ajouter comme on l'a fait dans l'exemple que nous traitons un peu plus bas.

On fait usage de cette méthode pour trouver les chiffres de la racine successivement. Supposons, par exemple, la racine comprise entre 2 et 3; on diminuera les racines de deux

unités; on cherchera la première décimale de la racine : on réduit pour cela l'équation à ses deux derniers termes; si l'on trouve que cette décimale est 5, on diminuera les racines de 0,5 et l'on continuera ainsi de suite; il peut arriver que, en procédant ainsi, on trouve un chiffre trop fort pour la décimale cherchée; on en sera averti, parce que, dans l'équation transformée, la nouvelle racine est négative; alors on essaye un chiffre moins élevé; si l'on a trouvé un chiffre trop faible, la suite du calcul ne tarde pas à mettre le fait en évidence.

Comme exemple, nous reprendrons l'équation étudiée plus haut

$$x^3 - 7x + 7 = 0.$$

Cherchons la racine comprise entre 1,3 et 1,4; le calcul se dispose ainsi :

$$\begin{array}{cccc}
1 & 0 & -7 & +7 \\
1 & 1 & -6 & +1 \\
1 & 2 & -4 & \\
1 & 3 & & \\
 & \underline{0,3} & \underline{0,99} & \underline{-0,903} \\
1 & 3,3 & -3,01 & 0,097 \\
 & \underline{0,3} & \underline{1,08} & \\
1 & 3,6 & -1,93 & \\
 & \underline{0,3} & & \\
1 & 3,9 & & \\
1 & & &
\end{array}$$

La racine a été diminuée de 1,3; le chiffre suivant est déterminé par l'équation

$$1,93x = 0,067, \qquad x = 0,05;$$

on diminue alors la racine de 0,05

$$\begin{array}{cccc}
1 & 3,9 & -1,93 & 0,097 \\
 & \underline{0,05} & \underline{0,1975} & \underline{-0,086625} \\
 & 3,95 & -1,7325 & 0,010375 \\
 & \underline{0,05} & \underline{0,20} & \\
 & 4,00 & -1,5325 & \\
 & \underline{0,05} & & \\
 & 4,05 & &
\end{array}$$

les deux derniers termes donnent alors le chiffre 6; ainsi

1	4,05	—1,5325	0,010375
	0,006	0,024336	—0,009048984
	4,056	—1,508164	0,001326016
	0,006	0,024372	
	4,062	—1,483792	
	0,006		
	4,068		

d'où l'on déduit le chiffre suivant 8.

139. Lorsque l'on a ainsi trouvé quelques chiffres, on peut trouver plusieurs des suivants par une méthode abrégée; on voit, par exemple, que, pour trouver le chiffre 8, il n'est pas nécessaire de faire usage des quatre dernières décimales des deux dernières séries; on laisse de côté les deux derniers chiffres de la première série et les chiffres correspondants des séries suivantes.

Calcul des racines imaginaires.

140. Il a été prouvé (**110**) que l'on pouvait séparer les racines imaginaires en cherchant des limites pour les modules et les arguments de ces racines, ou en cherchant des limites entre lesquelles sont comprises la partie réelle et la partie purement imaginaire. Ensuite, on peut utiliser la méthode de Newton pour déterminer plus complètement les racines. En général, le calcul présentera de grandes difficultés, car l'on n'a pas de moyen commode pour s'assurer que l'on approche effectivement de la racine; aussi vaut-il mieux employer un autre moyen, et l'on ramène la recherche des racines imaginaires à la recherche des racines réelles d'une autre équation.

Soit

$$f(x) = 0$$

l'équation à résoudre: posons

$$x = y + iz,$$

on a

$$f(y)+f'(y)\,iz-f''(y)\frac{z^2}{1.2}-f'''(y)\frac{z^3 i}{1.2.3}+\ldots=0,$$

équation qui se décompose en deux autres :

$$f(y)-f''(y)\frac{z^2}{1.2}+f^{\text{IV}}(y)\frac{z^4}{1.2.3.4}-\ldots=0,$$

et

$$f'(y)-f'''(y)\frac{z^2}{1.2.3}+f^{\text{V}}(y)\frac{z^4}{5!}-\ldots=0.$$

Si l'on élimine y entre ces deux équations, on obtient une équation en z, où z n'entre qu'avec des exposants pairs et qui, par conséquent, peut être abaissée. On déterminera, d'après les méthodes exposées plus haut, les valeurs positives de z^2; on sait que les méthodes d'élimination permettent d'exprimer y rationnellement en fonction de z; chaque valeur de z donnera une valeur correspondante de y, si nous supposons l'équation donnée à coefficients réels et qu'une seule paire de racines conjuguées ont la même partie imaginaire, en sorte qu'à une valeur de z^2 ne correspond qu'une valeur de y; si deux paires de racines ont la même partie imaginaire, une équation du second degré donnera les valeurs correspondantes de y, et ainsi de suite, conformément à ce qui a été dit dans la théorie de l'élimination.

On comprendra mieux l'esprit de cette méthode en la considérant à un autre point de vue. Soient x_1 et x_2 deux racines conjuguées, et soit

$$x_1=y_1+iz_1, \qquad x_2=y_1-iz_1,$$

lors

$$y_1=\frac{1}{2}(x_1+x_2),$$

$$z_1^2=-\frac{1}{4}(x_1-x_2)^2,$$

l'équation en z^2 est donc, à un léger changement de variable près, l'équation aux carrés des différences. Elle a une racine négative correspondant à chaque couple de racines imagi-

naires de la proposée, une racine réelle correspondant à une combinaison de deux racines réelles, et une racine imaginaire correspondant à chaque combinaison d'une racine réelle et d'une racine imaginaire, ou de deux racines imaginaires non conjuguées.

Exemple :

$$x^4 + ax^2 + bx + c = 0,$$

on trouve

$$y^4 + ay^2 + by + c - (6y^2 + a)z^2 + z^4 = 0,$$

$$4y^3 + 2ay + b - 4yz^2 = 0,$$

et, en éliminant z^2,

$$y^6 + \frac{a}{2}y^4 + \frac{a^2 - 4c}{16}y^2 - \frac{b^2}{64} = 0,$$

$$z^2 = y^2 + \frac{a}{2} + \frac{b}{4y}.$$

Pour

$$x^4 - x + 1,$$

on a les deux équations

$$y^6 - \frac{1}{4}y^2 - \frac{1}{64} = 0, \qquad z^2 = y^2 - \frac{1}{4y}.$$

Si l'on pose

$$y^2 = \frac{v}{4},$$

on a

$$v^3 - 4v - 1 = 0,$$

ou, en diminuant de 2 les racines,

$$v_1^3 + 6v_1^2 + 8v_1 - 1 = 0,$$

en faisant usage d'un développement en série récurrente, l'échelle de relation est

$$8, \quad 6, \quad 1,$$

et l'on trouve

$$1,\quad 8,\quad 70,\quad 609,\quad 5300,\quad 46124\ldots$$

$$\rho = 2 + \frac{5300}{46124} = 2,1149076\ldots,$$

$$y^2 = 0,5287269\ldots.\qquad y = \pm 0,727136\ldots,$$

$$z^2 = \begin{cases} 0,8725415, \\ 0,1849123, \end{cases}$$

et, par suite, les quatre racines sont

$$-0,727136\ldots \pm i.0,934092\ldots,$$
$$+0,727136\ldots \pm i.0,430014\ldots.$$

QUATRIÈME PARTIE.

SUR LES SUBSTITUTIONS.

CHAPITRE I.

DES SUBSTITUTIONS EN GÉNÉRAL.

Ordre des substitutions.

141. Si l'on considère une fonction de x_1, x_2, x_3, par exemple

$$x_1 + 2x_2 + 3x_3,$$

on peut en déduire une autre

$$x_2 + 2x_3 + 3x_1,$$

en remplaçant x_1 par x_2, x_2 par x_3 et x_3 par x_1. L'opération par laquelle on remplace ainsi plusieurs lettres par d'autres est ce qu'on appelle une *substitution :* on représente cette opération au moyen de deux séries de lettres, chaque lettre placée au-dessus d'une autre indiquant qu'elle doit être substituée à cette autre ; la substitution que nous avons effectuée ci-dessus pourra donc être représentée par le symbole

$$\begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

et, comme l'ordre dans lequel s'effectuent les remplacements est indifférent, on peut sans inconvénient remplacer le symbole précédent par un autre obtenu en intervertissant l'ordre des lettres pourvu que les lettres placées dans une même colonne verticale restent dans une même colonne.

La forme la plus générale d'une substitution de n lettres est alors

$$S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}$$

où A_1 et A_0 représentent des permutations différentes de n lettres. A_1 est le *numérateur*, A_0 le *dénominateur* de la substitution. La lettre qui en remplace une autre sera dite la *remplaçante* de cette autre.

Si on laisse A_0 inaltéré, on pourra remplacer A_1 par $n!$ permutations, on a donc en tout $n!$ substitutions de n lettres; l'une d'elles

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}$$

qui laisse toutes les lettres en place se représente par le nombre 1.

Lorsque dans une substitution, au-dessus l'une de l'autre, figurent deux lettres identiques, on peut en faire abstraction et la substitution n'est en réalité qu'une substitution entre un moins grand nombre de lettres que n.

Le symbole

$$SA_0$$

exprime que la substitution S s'effectue sur l'arrangement A_0, ainsi

$$\begin{pmatrix} A_1 \\ A_0 \end{pmatrix} A_0 = A_1.$$

Le produit de deux substitutions

$$TS$$

représente la substitution qui résulte de la substitution S effectuée d'abord et de la substitution T effectuée ensuite; par exemple, on a

$$\begin{pmatrix} A_2 \\ A_1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}$$

et l'ordre des facteurs ici n'est pas indifférent. Si l'on effectue p fois de suite la substitution S, on a une substitution finale que l'on représente par S^p; alors

$$S^0 = 1,$$

S^0 et 1 signifiant qu'on laisse toutes les lettres en place. Si

l'on a

$$S = T,$$

on a évidemment

$$SS_1 = TS_1, \qquad S_1 S = S_1 T;$$

en sorte que l'on peut multiplier à gauche ou à droite les deux membres d'une égalité par une même substitution.

Exemple :

$$x_1 x_2^2 + x_3^3 x_4,$$

par la substitution

$$S = \begin{pmatrix} x_4 & x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

devient

$$x_4 x_1^2 + x_2^3 x_3,$$

soit

$$T = \begin{pmatrix} x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix},$$

on aura

$$ST = \begin{pmatrix} x_2 & x_4 & x_1 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}, \qquad TS = \begin{pmatrix} x_4 & x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

$$S^2 = \begin{pmatrix} x_3 & x_4 & x_1 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}, \qquad T^2 = \begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}, \qquad \cdots\cdot$$

142. Si l'on considère la suite des substitutions

$$1, \qquad S, \qquad S^2, \qquad \ldots,$$

le nombre total des substitutions de n lettres étant fini, on doit nécessairement retomber sur une substitution déjà obtenue : supposons, par exemple, que l'on trouve alors

$$S^{\alpha+\beta} = S^\alpha$$

ou

$$S^\beta S^\alpha = S^\alpha,$$

cette formule prouve que la substitution S^β laisse invariable une permutation quelconque; ainsi

$$S^\beta = 1$$

et k désignant un entier quelconque

$$S^{k\beta+\alpha} = S^\alpha;$$

les puissances successives de S forment donc une suite périodique.

Si β *est le plus petit entier donnant* $S^\beta = 1$, *on dit que* S *est d'ordre* β.

Si au lieu de $S^{\beta-\alpha}$ on écrit $S^{-\alpha}$; on a

$$S^{-\alpha} S^\alpha = 1.$$

On voit facilement que si S remplace la permutation a par la permutation b, S^{-1} remplacera b par a.

Soit β l'ordre de S et

$$\beta = f\beta_1, \qquad \alpha = f\alpha_1;$$

f désignant le plus grand commun diviseur de α et β. α_1 et β_1 seront premiers entre eux. Pour déterminer l'ordre x de la substitution S^α posons

$$(S^\alpha)^x = 1 = S^{k\beta},$$

d'où

$$x = \frac{k\beta}{\alpha} = \frac{k\beta_1}{\alpha_1},$$

il en résulte que β_1 ou $\frac{\beta}{f}$ est la plus petite valeur de x, donc :

Si S *est d'ordre* β, S^α *sera d'ordre* $\frac{\beta}{f}$, f *étant le plus grand commun diviseur* de α *et* β. *On remarquera que* S^α et S *sont de même ordre si* α *et* β *sont premiers entre eux*. Dans ce cas, les puissances de S^α seront égales, à l'ordre près, à celles de S ; par exemple, si l'on pose

$$(S^\alpha)^x = S^p = S^{\beta y+p},$$

on aura

$$\alpha x - \beta y = p,$$

équation qui a toujours une solution si α et β sont premiers entre eux.

Exemple. — Soit

$$S = \begin{pmatrix} e & a & c & b & d \\ a & b & c & d & e \end{pmatrix} = \begin{pmatrix} e & a & b & d \\ a & b & d & e \end{pmatrix},$$

on a

$$S^2 = \begin{pmatrix} d & e & a & b \\ a & b & d & e \end{pmatrix},$$

$$S^3 = \begin{pmatrix} b & d & e & a \\ a & b & d & e \end{pmatrix},$$

$$S^4 = \begin{pmatrix} a & b & d & e \\ a & b & d & e \end{pmatrix} = 1,$$

et S est du quatrième ordre; si l'on pose, par exemple,

$$(S^3)^x = S^2 = S^{4y+2},$$

on a

$$3x - 4y = 2; \qquad x = 2,$$

et l'on a aussi

$$(S^3)^2 = \begin{pmatrix} d & e & a & b \\ a & b & d & e \end{pmatrix} = S^2.$$

Si l'on applique cette substitution à la fonction

$$a^3 + 3ab^2 - 2cde,$$

on a

$$d^3 + 3de^2 - 2cab.$$

Substitutions circulaires.

143. Une substitution est dite *circulaire*, quand elle substitue à chaque lettre du dénominateur celle qui la suit et quand elle remplace la dernière par la première.

La substitution

$$\begin{pmatrix} e & a & b & d \\ a & b & d & e \end{pmatrix}$$

est circulaire, car elle remplace chaque lettre de $a\ b\ d\ e$ par la suivante et la dernière e par a; une pareille substitution se représente encore par une suite de lettres entre paren-

thèses, ainsi

$$S = \begin{pmatrix} b & c & d & e & a \\ a & b & c & d & e \end{pmatrix} = (a\ b\ c\ d\ e) = (b\ c\ d\ e\ a), \qquad \ldots.$$

L'ordre d'une substitution circulaire est évidemment égal au nombre des lettres qu'elle déplace. Car, par une application répétée de cette substitution, on remplace successivement a par $b\ c\ d\ e\ a$ et, quand on a remplacé a par a, on obtient la substitution 1.

144. *Toute substitution est un produit de substitutions circulaires.*

Prenons, en effet, une lettre arbitrairement au dénominateur de cette substitution, elle se trouve remplacée par une seconde, celle-ci par une troisième et ainsi de suite jusqu'à ce que l'on tombe sur la première; ces lettres constituent une substitution circulaire ou un *cycle*. Si l'on opère de la même façon sur les autres lettres, on obtient de nouveaux cycles. Une substitution ou un cycle qui opère sur deux lettres est ce que l'on appelle une *transposition;* elle revient à l'échange de ces lettres; un cycle composé d'une seule lettre peut être négligé.

La substitution

$$S = \begin{pmatrix} h & k & d & f & b & j & a & g & e & c & i & m & l & n \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n \end{pmatrix}$$

peut se décomposer ainsi

$$S = (a\ h\ g)\,(b\ k\ i\ e)\,(c\ d\ f\ j)\,(l\ m)\,(n),$$

où le dernier cycle formé d'une seule lettre peut être laissé de côté. Il est évident que l'ordre dans lequel on écrit les cycles est indifférent.

145. *L'ordre d'une substitution est égal au plus petit multiple des ordres de ses cycles.*

Soit, en effet,

$$S = c_0 c_1 c_2 \ldots$$

une substitution décomposée en ses facteurs circulaires, et soit

$$S^x = 1;$$

comme les cycles sont relatifs à des lettres différentes, on a

$$c_0^x = 1, \quad c_1^x = 1, \quad c_2^x = 1, \quad \ldots.$$

La plus petite valeur que puisse prendre x est, d'après cela, le plus petit des nombres satisfaisant à la fois aux égalités précédentes.

Si tous les cycles de S sont de même ordre, cet ordre sera aussi celui de S, et une pareille substitution est dite *régulière;* il ne faut pas oublier que les cycles considérés doivent tous contenir des lettres différentes.

$(ab)(cd)$ est une substitution régulière du second ordre, mais $(ab)(bc) = (abc)$ est une substitution circulaire du troisième ordre.

146. *Si* S *est une substitution circulaire d'ordre* β, S^α *sera une substitution régulière composée de f cycles, f désignant le plus grand commun diviseur de* α et β. Si α et β sont premiers entre eux, S^α sera elle-même circulaire.

Soit

$$S = (a_1 \ a_2 \ \ldots \ a_\beta);$$

S remplace a_p par a_{p+1}, S^2 remplace a_p par a_{p+2}, ..., S^α remplace a_p par $a_{p+\alpha}$; si l'on effectue la substitution S^α, on obtiendra d'abord un cycle

$$(a_p \ a_{p+\alpha} \ a_{p+2\alpha} \ \ldots),$$

ou un indice tel que $p + x\alpha$ devra être remplacé par le reste de sa division par β, s'il est plus grand que β. Alors, pour retomber sur la lettre a_p, il faut que

$$p + \alpha x = p + \beta y \quad \text{ou} \quad x = \frac{\beta y}{\alpha},$$

où x désigne le nombre des lettres du cycle. Si α et β sont premiers entre eux $y = \alpha$, $x = \beta$, et la substitution S est cir-

culaire. Si $\alpha = f\alpha_1$, $\beta = f\beta_1$, alors $y = \frac{\alpha}{f}$ et le nombre des cycles est

$$\frac{\beta}{x} = f.$$

Exemple :

$$\begin{aligned} S &= (abcdef), \\ S^2 &= (ace)(bdf), \\ S^3 &= (ad)(be)(cf), \\ S^4 &= (aec)(bfd), \\ S^5 &= (afedcb), \\ S^6 &= 1. \end{aligned}$$

147. *Toute substitution régulière est une puissance d'une substitution circulaire.*

Soit la substitution régulière

$$S = (a_1 b_1 c_1 \ldots g_1)(a_2 b_2 c_2 \ldots g_2) \ldots (a_m b_m c_m \ldots g_m).$$

Si l'on pose

$$C = (a_1 a_2 \ldots a_m b_1 b_2 \ldots b_m \ldots g_1 g_2 \ldots g_m),$$

on a évidemment

$$S = C^m.$$

148. *Toute substitution peut être décomposée en facteurs primitifs,* c'est-à-dire en facteurs dont l'ordre est un nombre premier ou une puissance d'un nombre premier.

Supposons S d'ordre n et

$$n = \alpha\beta,$$

α et β désignant des nombres premiers entre eux. On peut toujours trouver des entiers x, y tels que

$$\alpha x + \beta y = 1.$$

Alors

$$S = S^{\alpha x} S^{\beta y}.$$

Or, on a

$$(S^{\alpha x})^\beta = 1, \qquad (S^{\beta y})^\alpha = 1,$$

de sorte que les facteurs $S^{\alpha x}$, $S^{\beta y}$ sont d'ordre β et α respectivement; on peut ainsi poursuivre la décomposition en facteurs jusqu'à ce que l'on n'ait plus que des facteurs d'un ordre égal à un nombre premier, ou à une puissance d'un nombre premier.

Exemple :

$$S = (abcdef)$$

est d'ordre $2 \times 3 = 6$; on a donc

$$S = S^3 S^4,$$

où

$$S^3 = (ad)(be)(cf),$$
$$S^4 = (aec)(bfd).$$

Substitutions semblables et échangeables.

149. Deux substitutions sont *semblables,* quand elles sont composées d'un même nombre de cycles composés d'un même nombre de lettres. Deux substitutions S et T sont *échangeables* quand on a

$$ST = TS.$$

La substitution

$$ASA^{-1}$$

est dite la *transformée de* S *par* A.

150. *Une substitution est semblable à ses transformées.*

Soit

$$(abc\ldots)$$

un des cycles de S et a_1, b_1, c_1, ... les lettres par lesquelles A remplace a, b, c, ...; quand on opère la substitution A^{-1}, a_1 se trouve remplacé par a, qui se trouve remplacé par b par la substitution S, qui se trouve lui-même remplacé par b_1 par la substitution A. La substitution ASA^{-1} remplace donc a_1 par b_1, b_1 par c_1, ..., de sorte qu'au cycle $(abc\ldots)$ correspond, dans la transformée, le cycle $(a_1 b_1 c_1 \ldots)$; donc :

La transformée de S *par* A *peut s'obtenir en effectuant sur les lettres des cycles de* S *la substitution* A.

Exemple :

$$S = (abcd), \qquad A = (ac)(bd), \qquad ASA^{-1} = (cdab).$$

Si

$$S = (abc)(de),$$
$$T = (dca)(be),$$

on a

$$T = ASA^{-1},$$

où

$$A = (adbc).$$

Ainsi *quand* S *et* T *sont semblables, on peut toujours trouver une substitution* A *qui transforme* S *en* T. Cette substitution est celle qui remplace chaque lettre de S par celle qui occupe la même place dans T.

151. *Les deux produits de deux substitutions sont semblables.* ST et TS sont semblables, car

$$ST = S(TS)S^{-1}.$$

152. *La transformée d'un produit est égale au produit des transformées de ses facteurs.* Ainsi

$$A(ST)A^{-1} = ASA^{-1}ATA^{-1}.$$

153. *Si deux substitutions sont échangeables, leurs transformées le sont.*

En effet, si

$$ST = TS,$$

$$ASA^{-1}ATA^{-1} = ATA^{-1}ASA^{-1}.$$

154. Si les substitutions S et T sont échangeables, on a

$$ST = TS \qquad \text{ou} \qquad S = TST^{-1},$$

et S est égale à sa transformée par T.

Pour effectuer la transformation de S par T, il faut (150)

effectuer la substitution T dans les cycles de S; alors deux cas pourront se présenter : ou bien T ne modifiera pas les cycles de S, ou bien elle se bornera à les échanger entre eux. Le premier cas se présentera si les lettres d'un cycle de S n'entrent pas dans T ou si une puissance d'un cycle est un facteur de T, ce qui fera que le cycle transformé commence par une autre lettre sans que l'ordre des lettres soit altéré. En dehors de ces facteurs, T ne peut contenir que des facteurs qui peuvent échanger des cycles de S; cherchons un pareil facteur Q.

Si l'on applique ce facteur au cycle C_1, celui-ci se change en un autre C_2 qui doit aussi entrer dans S, C_2 se change en C_3, ..., C_μ se change en C_1; d'ailleurs C_1 gagné par la transformation peut commencer avec une autre lettre que dans S; on a, par exemple,

$$\begin{aligned} C_1 &= (a_1 a_2 \ldots a_i), \\ C_2 &= (b_1 b_2 \ldots b_i), \\ &\ldots\ldots\ldots\ldots\ldots, \\ C_\mu &= (f_1 f_2 \ldots f_i), \end{aligned}$$

et C_1 devient

$$(a_{\rho+1} a_{\rho+2} \ldots a_\rho).$$

Le facteur P de S

$$P = C_1 C_2 \ldots C_\mu$$

est une substitution régulière et, si $\rho = 0$, le facteur Q de T

$$Q = (a_1 b_1 \ldots f_1)(a_2 b_2 \ldots f_2)\ldots(a_i b_i \ldots f_i)$$

est régulier. Q est encore régulier si ρ n'est pas nul, mais le nombre des lettres dans chaque cycle sera un multiple de μ; le premier cycle, quand on prend les indices suivant le module i, devient

$$(a_1 b_1 \ldots f_1 a_{\rho+1} b_{\rho+1} \ldots f_{\rho+1} a_{2\rho+1} \ldots),$$

dans lequel on parvient à un terme

$$a_{q\rho+1},$$

qui est identique à a_1; alors on doit avoir

$$q\rho = ki,$$

ou, en appelant α le plus grand commun diviseur de ρ et de i, et en posant $\alpha\rho_1 = \rho$, $\alpha i_1 = i$,

$$q\rho_1 = ki_1;$$

donc

$$q = i_1;$$

Q est donc un produit de α facteurs circulaires composés chacun de $i_1\mu$ lettres, et l'on a

$$P^\rho = (a_1 a_{1+\rho} a_{1+2\rho} \ldots)(b_1 b_{1+\rho} b_{1+2\rho} \ldots)\ldots,$$
$$Q^\mu = (a_1 a_{1+\rho} a_{1+2\rho} \ldots)(b_1 b_{1+\rho} b_{1+2\rho} \ldots)\ldots,$$

d'où

$$P^\rho = Q^\mu,$$

les membres étant différents de l'unité, car P est d'ordre i et $\rho < i$. S et T seront donc échangeables, seulement si leurs lettres communes constituent des substitutions régulières satisfaisant à la condition précédente. L'équation $P^\rho = Q^\mu$ est une condition nécessaire, mais non suffisante pour que S et T soient échangeables.

155. *Il existe toujours des substitutions* T *satisfaisant à l'équation*

$$S^m = TST^{-1}, \tag{1}$$

lorsque m *est premier avec l'ordre de* S.

m doit être premier avec l'ordre de chacun des cycles de S. S^m est alors semblable à S, car chaque cycle, élevé à la puissance m, donne un nouveau cycle composé des mêmes lettres. Alors (150) il y aura des substitutions T. Soit T_1 l'une d'elles, (1) pourra s'écrire

$$T_1 S T_1^{-1} = TST^{-1}$$

ou

$$ST_1^{-1}T = T_1^{-1}TS.$$

S et $T_1^{-1}T$ sont alors échangeables. Soit U une substitution quelconque échangeable avec S, et soit

$$T_1^{-1}T = U,$$

d'où

$$T = T_1 U.$$

Cette substitution satisfait à (1), car

$$T_1 U S (T_1 U)^{-1} = T_1 S T_1^{-1} = S^m;$$

on voit donc que l'*on obtient toutes les solutions de* (1) *en multipliant une solution particulière par les substitutions échangeables avec* S.

Exemple :

$$S = (abc)(def); \qquad S^2 = (acb)(dfe);$$
$$S^2 = TST^{-1}, \qquad \text{si} \qquad T = (bc)(ef).$$

Substitutions positives et négatives.

156. *Une substitution quelconque peut être décomposée en un produit de transpositions.*

En effet, on peut, au moyen d'une transposition, amener une lettre à la place qu'elle doit occuper définitivement; et l'on peut alors remplacer la substitution par une autre dans laquelle n'apparaît plus cette lettre; la nouvelle substitution pourra être traitée comme la première, et ainsi de suite. On a ainsi, par exemple,

$$(abcd) = (bd)(bc)(ad).$$

157. *Si le produit d'un certain nombre de transpositions est égal à* 1, *le nombre de ces transpositions est pair.*

Soient $a, b, c, d, \ldots$ les lettres sur lesquelles on opère; considérons le produit

$$(a-b)(a-c)(a-d)\ldots(b-c)(b-d)\ldots:$$

il change de signe par une transposition quelconque. Soient p, q, r des trois lettres, dans le produit entreront les facteurs $\pm(p-r)$ et $\pm(q-r)$, dont le produit ne change pas par la transposition (pq). Les facteurs du produit considéré chan-

gent donc de signe par couples; abstraction faite de $p - q$, qui se change en $q - p$, le produit tout entier change donc de signe par la transposition (pq). Si donc le produit des transpositions employées est égal à 1, il faut que le produit des différences considérées ait changé de signe un nombre pair de fois, c'est-à-dire que le nombre des transpositions en question soit pair.

Quelle que soit la manière dont une substitution a été décomposée en un produit de transpositions, le nombre de ces transpositions est toujours de même parité.

En effet, supposons qu'un produit de m transpositions soit égal à un produit de n transpositions. Si l'on multiplie ces deux produits successivement par les n transpositions, on obtiendra un produit de $m+n$ transpositions égal à 1; donc $m+n$ est pair et, par suite, m et n sont de même parité.

On est donc conduit à considérer deux classes de substitutions : les unes sont un produit d'un nombre pair de transpositions; les autres sont un produit d'un nombre impair de transpositions; les premières sont dites *positives*, les autres sont dites *négatives*, parce qu'elles ne changent pas ou changent le signe du produit de différences. On voit facilement qu'une substitution circulaire est positive quand elle opère sur un nombre impair de lettres, et qu'elle est négative quand elle opère sur un nombre pair de lettres. Si une substitution est décomposable en μ cycles de $n_1, n_2, \ldots, n_\mu$ lettres respectivement, son signe sera celui de

$$(-1)^{n_1+n_2+\ldots+n_\mu-\mu},$$

de sorte que la différence entre le nombre des lettres et celui des cycles sera pair ou impair, suivant que la substitution sera positive ou négative.

CHAPITRE II.

SUBSTITUTIONS CONJUGUÉES OU GROUPES.

Théorème de Lagrange.

158. On dit que des substitutions forment un *groupe* ou un système conjugué, lorsque le produit de deux quelconques de ces substitutions fait partie de leur système. Les puissances d'une même substitution, par exemple, forment un groupe. Les substitutions en nombre $n!$ que l'on peut former avec n lettres forment également un groupe (le groupe général). Pour exprimer que le groupe G est formé des substitutions $1, S_1, S_2, \ldots$, on écrit

$$G = (1, S_1, S_2, \ldots).$$

Le nombre des substitutions d'un groupe est l'*ordre* de ce groupe, le nombre des lettres sur lesquelles il opère est son degré; l'ordre du groupe formé des puissances de S est égal à l'ordre de S.

159. *Si un groupe* Γ *d'ordre* μ *est contenu dans un groupe* G *d'ordre* m, μ *est un diviseur de* m (Théorème de Lagrange).

Supposons le premier groupe Γ formé des substitutions

$$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{\mu-1},$$

soit T_1 une autre substitution de G, ce groupe G contiendra les substitutions

$$T_1, \quad S_1 T_1, \quad S_2 T_1, \quad \ldots, \quad S_{\mu-1} T_1;$$

si G contient encore d'autres substitutions, soit T_2 l'une d'elles, il contiendra

$$T_2, \quad S_1T_2, \quad S_2T_2, \quad \ldots, \quad S_{\mu-1}T_2;$$

et ainsi de suite. On obtient ainsi les substitutions de G ordonnées en des séries contenant chacune μ substitutions et le théorème sera démontré, si l'on constate que toutes ces substitutions sont différentes. S'il n'en était pas ainsi, on aurait

$$S_\alpha T_\beta = S_{\alpha_1} T_{\beta_1}$$

pour certaines valeurs de α, β, α_1, β_1. Soit $\beta > \beta_1$, on aurait

$$T_\beta = S_\alpha^{-1} S_{\alpha_1} T_{\beta_1},$$

ce qui est impossible; en effet, le second membre fait partie des substitutions

$$T_{\beta_1}, \quad S_1T_{\beta_1}, \quad \ldots, \quad S_{\mu-1}T_{\beta_1}$$

et T_β ne fait précisément pas partie de ces substitutions.

On verrait de même que les substitutions du groupe G peuvent être ordonnées en séries de la forme

$$T_\alpha, \quad T_\alpha S_1, \quad T_\alpha S_2, \quad \ldots, \quad T_\alpha S_{\mu-1}.$$

Du théorème que nous venons de démontrer on tire les conséquences suivantes qui sont très importantes :

L'ordre d'un groupe de degré n est un diviseur de n!

Car ce groupe est contenu dans le groupe général.

L'ordre d'un groupe est divisible par l'ordre d'une quelconque de ses substitutions.

Car il contient le groupe formé des puissances d'une quelconque de ses substitutions.

Un groupe dont l'ordre est un nombre premier p ne contient que des substitutions régulières d'ordre p (excepté la substitution 1). *Si son degré est p, le groupe se compose des p puissances d'une substitution circulaire d'ordre p.*

On voit aussi que

Les substitutions communes à deux groupes forment un groupe.

Car le produit de deux de ces substitutions appartient aux deux groupes.

Les substitutions d'un groupe qui ne déplacent pas des lettres données forment un groupe.

Car si certaines lettres ne sont pas déplacées par deux substitutions elles ne le sont pas non plus par leur produit.

Toutes les substitutions d'un groupe qui sont échangeables avec une substitution donnée forment un groupe.

Substitutions permutables avec un groupe.

160. *Les transformées des substitutions*

$$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{m-1}$$

d'un groupe G *par une substitution quelconque* T *forment elles-mêmes un groupe.*

En effet,

$$TS_1T^{-1}TS_2T^{-1} = T(S_1S_2)T^{-1}.$$

Les substitutions des deux groupes sont semblables deux à deux, et dans ce cas on dit que les deux groupes eux-mêmes sont *semblables*.

Lorsque le groupe transformé coïncide avec le groupe primitif on dit que la substitution T est *permutable* avec le groupe G. Dans ce cas, on a, pour chaque valeur de α, une valeur de β telle que

$$TS_\alpha = S_\beta T.$$

Toutes les substitutions d'un groupe G, *qui sont permutables avec un groupe* H *forment un groupe.*

En effet, si U et T sont permutables avec $H = (1, S_1, S_2, \ldots)$ on a

$$UTS_\alpha(UT)^{-1} = UTS_\alpha T^{-1}U^{-1} = US_\beta U^{-1} = S_\gamma,$$

de sorte que UT est aussi permutable avec H.

161. Un groupe est *simple*, quand il ne contient aucun groupe avec lequel toutes ses substitutions sont permutables, dans le cas contraire il est *composé*.

Soit G un groupe composé qui contient le groupe H avec lequel toutes ses substitutions sont permutables; soient

$$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{m-1}$$

les substitutions de H, soit T une substitution de G qui ne soit pas contenue dans H; H peut contenir des puissances de T, soit T^α la puissance la moins élevée de T contenue dans H, les substitutions de la forme

$$T^\beta S_k$$

sont contenues dans G et sont différentes pour $\beta < \alpha$; pour $\beta = \alpha$, on obtient les substitutions de H, et pour $\beta > \alpha$, on obtient périodiquement les mêmes substitutions que tout à l'heure, et les substitutions de H quand β est un multiple de α. L'ordre de T doit donc être un multiple de α.

Les αm substitutions que nous venons d'obtenir forment un groupe H_1; en effet, on voit que le produit de deux quelconques d'entre elles appartient à la suite de ces αm substitutions, car pour une certaine valeur de h on a

$$T^\beta S_k = S_h T^\beta.$$

Sur la formation de quelques groupes.

162. *Les substitutions qui transforment* T *en une de ses puissances forment un groupe.*

En effet, si α et β sont premiers avec l'ordre μ de T et si l'on a

$$MTM^{-1} = T^\alpha, \quad NTN^{-1} = T^\beta,$$

on a aussi

$$(MN)T(MN)^{-1} = MNT\ldots M^{-1} = MT^\beta M^{-1} = MTM^{-1}MTM^{-1}N^{-1} = T^{\alpha\beta};$$

de sorte que MN fait partie des substitutions considérées si M et N en font partie.

On peut voir que l'on obtient encore un groupe, si, parmi

les substitutions du groupe considéré, on ne prend que celles dans lesquelles *les exposants de* T *satisfont à une certaine condition* si cette condition est telle que $\alpha\beta$ y satisfait quand α et β y satisfont, $\alpha\beta$ étant pris suivant le module μ; cela a lieu non seulement quand α et β sont premiers avec μ, mais encore quand, α et β étant premiers avec μ, ils satisfont à la congruence

$$x^\theta \equiv k^m \pmod{\mu},$$

où θ et k sont des nombres donnés, le second premier avec μ, m étant quelconque.

En effet, si l'on a

$$\alpha^\theta \equiv k^{m_1}; \qquad \beta^\theta \equiv k^{m_2},$$

on a

$$(\alpha\beta)^\theta \equiv k^{m_1+m_2}.$$

Considérons, par exemple, une substitution circulaire T de μ lettres, prenons pour α et β tous les nombres premiers avec μ; le nombre de ces entiers est $\varphi(\mu)$; considérons les $\varphi(\mu)$ puissances de T dont l'exposant est premier à μ, et inférieur à μ, chacune d'elles peut être formée par transformation de T, et fournir μ substitutions, car chaque lettre de la puissance de T peut être placée la première. On obtient ainsi un groupe de $\mu\varphi(\mu)$ substitutions, et si μ est un nombre premier p l'ordre de ce groupe sera $p(p-1)$. On pourrait aussi se borner à considérer les substitutions que l'on obtient quand on écrit T et ses puissances de manière qu'elles commencent avec la même lettre; cette lettre ne figure pas alors dans les substitutions cherchées, et celles-ci sont alors des substitutions de $\mu - 1$ lettres et forment un groupe d'ordre $\varphi(\mu)$.

Exemple I :

$$T = (a\ b\ c\ d\ e\ f), \qquad T^5 = (a\ f\ e\ d\ c\ b).$$

La transformation se fait par

$$M = \begin{pmatrix} a & f & e & d & c & b \\ a & b & c & d & e & f \end{pmatrix} = (b\ f)(c\ e),$$

qui avec 1 forme un groupe du second ordre.

Si l'on écrit T^5 de toutes les manières possibles, on obtient un groupe du douzième ordre qui contient le précédent.

Exemple II :

$$\begin{aligned} T &= (a\ b\ c\ d\ e), \\ T^2 &= (a\ c\ e\ b\ d), \\ T^3 &= (a\ d\ b\ e\ c), \\ T^4 &= (a\ e\ d\ c\ b). \end{aligned}$$

Si a conserve sa place dans la transformation, on obtient le groupe du quatrième ordre

$$1,\quad (b\ c\ e\ d),\quad (b\ d\ e\ c),\quad (b\ e),\quad (c\ d).$$

On a vu que si μ désignait un nombre premier p on obtenait un groupe de $p-1$ lettres d'ordre $p-1$; ce groupe se compose des puissances d'une substitution circulaire d'ordre $p-1$, s'il entre une pareille substitution dans le groupe. On peut poser

$$T = (a_0,\ a_1\ a_2\ \ldots\ a_{p-1}),\quad T^r = (a_0\ a_r\ a_{2r}\ \ldots),$$

et on obtient la transformante

$$U = \begin{pmatrix} a_0 & a_r & a_{2r} & \ldots \\ a_0 & a_1 & a_2 & \ldots \end{pmatrix} = (a_1\ a_r\ a_{r^2}\ \ldots),$$

qui est circulaire si r est racine primitive de p, ce qu'on peut supposer, puisque tout nombre premier a des racines primitives ; le groupe cherché est alors

$$1,\quad U,\quad U^2,\quad \ldots,\quad U^{p-2}.$$

Si l'on veut former le groupe d'ordre $p(p-1)$, on écrira T^r en le faisant commencer par chacune de ses lettres ; les transformantes ont alors la forme

$$T^h U^k,$$

car on obtient par une transformation par U^k la puissance demandée de T commençant par a_0, et avec une transformation par T^h on amènera une autre lettre à la première place. Par exemple,

$$T = (a\ b\ c\ d\ e),\quad T^3 = (b\ e\ c\ a\ d)$$

et l'on obtient la transformante

$$\begin{pmatrix} b & e & c & a & d \\ a & b & c & d & e \end{pmatrix} = \begin{pmatrix} b & e & c & a & d \\ a & d & b & e & c \end{pmatrix} \begin{pmatrix} a & d & b & e & c \\ a & b & c & d & e \end{pmatrix} = \mathrm{T}(b\ d\ e\ c);$$

on obtient ainsi le groupe cherché, en multipliant les puissances de U à gauche par les puissances de T.

Si l'on multiplie à droite on obtient les mêmes substitutions, mais dans un ordre différent.

Le groupe alterné.

163. *Parmi les* $\mathrm{N} = n!$ *substitutions que l'on peut former avec* n *lettres, celles qui sont positives forment un groupe d'ordre* $\frac{\mathrm{N}}{2}$ *et il n'y a pas d'autre groupe de cet ordre.*

Lorsqu'un groupe contient une substitution négative, il doit contenir autant de substitutions négatives que de substitutions positives. Si l'on multiplie toutes les substitutions de ce groupe par une de ses substitutions négatives on retrouve le groupe; comme cette multiplication change les substitutions négatives en substitutions positives et *vice versa*, il faut qu'il y en ait autant des unes que des autres; comme, d'ailleurs, les substitutions positives forment un groupe, il faut que toutes ces substitutions positives forment un groupe d'ordre $\frac{\mathrm{N}}{2}$. Ce groupe porte le nom de *groupe alterné*.

Considérons maintenant un groupe d'ordre $\frac{\mathrm{N}}{2}$ formé des substitutions $1, \mathrm{S}_1, \mathrm{S}_2, \ldots$; soit T une substitution quelconque qui ne fait pas partie du groupe, les $\frac{\mathrm{N}}{2}$ substitutions ST sont différentes entre elles et différentes de $1, \mathrm{S}_1, \mathrm{S}_2, \ldots$, les substitutions S et ST sont alors en nombre N et contiennent toutes les substitutions possibles : les substitutions S doivent donc renfermer et se confondre avec les substitutions $\mathrm{T}^2\mathrm{S}$ et de même avec les substitutions $\mathrm{T}^4\mathrm{S}$, $\mathrm{T}^6\mathrm{S}$, ...

Alors T doit être d'ordre pair, sans quoi TS devrait se trou-

ver dans le groupe considéré. Ce groupe devra alors contenir toutes les substitutions circulaires du troisième ordre et par suite le groupe alterné car on a

$$(a_1 a_2)(a_2 a_3) = (a_1 a_2 a_3), \qquad (a_1 a_2)(a_3 a_4) = (a_1 a_2 a_3)(a_2 a_3 a_4),$$

ce qui montre que toute substitution positive peut être mise sous la forme d'un produit de substitutions circulaires du troisième ordre.

Une fonction qui, sans être symétrique, n'est pas altérée par les substitutions du groupe alterné est dite *alternée*. Une pareille fonction n'a que deux valeurs, toute substitution ayant la forme S ou ST, S appartenant au groupe alterné et T désignant une substitution négative quelconque; puisque la fonction n'est pas altérée par les substitutions S, elle ne peut posséder qu'une valeur distincte d'une valeur donnée, valeur que lui fait acquérir la substitution T. Pour $n = 3$

$$y = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

est une fonction alternée qui prend les valeurs y et $-y$.

164. *Un groupe qui contient toutes les substitutions circulaires du troisième ordre est ou le groupe alterné ou le groupe général.*

Car on a vu qu'un pareil groupe contenait toutes les substitutions positives.

Un groupe qui contient toutes les substitutions circulaires d'ordre p est le groupe alterné ou le groupe général.

Car on a

$$(a_1 a_2 a_3) = (a_1 a_3 a_4 a_2 a_5 \ldots a_p)(a_p a_{p-1} \ldots a_5 a_2 a_1 a_4 a_3),$$

en sorte que le groupe contient toutes les substitutions circulaires du troisième ordre.

Groupes que l'on peut former par la multiplication des substitutions d'autres groupes.

165. Quand deux groupes

$$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{m-1},$$
$$1, \quad T_1, \quad T_2, \quad \ldots, \quad T_{n-1}$$

sont tels que

$$S_\alpha T_\beta = T_{\beta_1} S_{\alpha_1}$$

pour toutes les valeurs de α et β et pour des valeurs convenables de β_1 et α_1, on dit que ces groupes sont échangeables.

Si l'on multiplie toutes les substitutions S d'un même côté par toutes les substitutions T, on obtient un nouveau groupe d'ordre mn, si les groupes considérés n'ont d'autre substitution commune que l'unité.

En effet, toutes les substitutions obtenues ainsi sont différentes, car, si l'on pouvait avoir

$$S_\alpha T_\beta = S_{\alpha_1} T_{\beta_1},$$

on en conclurait

$$S_{\alpha_1}^{-1} S_\alpha = T_{\beta_1} T_\beta^{-1},$$

et les groupes auraient en commun une substitution qui, évidemment, est différente de l'unité. D'ailleurs

$$S_\alpha T_\beta S_{\alpha_1} T_{\beta_1},$$

par un échange de facteurs et d'indices convenables, peut être ramenée à la forme

$$S_\gamma T_\delta,$$

ce qui montre que nos mn substitutions forment un groupe.

Des théorèmes analogues peuvent être énoncés pour un grand nombre de groupes.

Théorème de Cauchy.

166. *Si p est un nombre premier, il existe un groupe de k lettres dont l'ordre est la plus haute puissance de p qui divise k!*

Si $k < p$, le groupe 1 d'ordre p^0 est le groupe dont il est question dans l'énoncé. Pour démontrer le théorème il suffit de montrer que s'il a lieu pour tous les nombres inférieurs à p^α il a encore lieu pour tous les nombres inférieurs à $p^{\alpha+1}$.

Tout nombre inférieur à $p^{\alpha+1}$ peut être mis sous la forme $pq + r$ où $q < p^\alpha$ et $r < p$; nous admettrons qu'avec les q lettres $a, b, c, \ldots$ on peut former un groupe d'ordre p^β où p^β est la plus haute puissance de p qui entre dans q!

Au moyen de chaque substitution $(abc\ldots)$, $(de\ldots)$, ... de ce groupe nous pouvons en former une autre

$$\begin{aligned}&(a_1 b_1 c_1 \ldots)(a_2 b_2 c_2 \ldots)\ldots(a_p b_p c_p \ldots)\\ \times\, &(d_1 e_1 \ldots)(d_2 e_2 \ldots)\ldots(d_p e_p \ldots)\\ \times\, &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

en remplaçant chaque cycle par un produit de p cycles composés des mêmes lettres affectées d'indices différents. Les substitutions ainsi obtenues forment un groupe de degré pq et d'ordre p^β; soit

$$T = (C_1, C_2 \ldots)$$

ce groupe; ses substitutions échangent les lettres sans toucher aux indices. Désignons les substitutions circulaires

$$(a_1 a_2, \ldots, a_p), \quad (b_1 b_2 \ldots, b_p), \quad \ldots$$

par

$$S_a, \quad S_b, \quad \ldots$$

respectivement. Ces substitutions échangent les indices sans modifier les lettres. Le groupe cherché est composé de substitutions de la forme

$$S_a^\gamma, \quad S_b^\delta, \quad \ldots, \quad C_\mu,$$

et leur nombre est $p^q p^\beta$. Nous allons montrer que toutes ces substitutions sont distinctes et qu'elles forment un groupe; on a, en effet, si C_μ remplace b par a,

$$S_a^\gamma C_\mu = C_\mu S_b^\gamma,$$

car les deux substitutions que l'on vient d'égaler remplacent

b_k par $a_{k+\gamma}$; on peut donc échanger des facteurs S et C dans un produit SC pourvu que l'on modifie convenablement l'indice de S. Si l'on pouvait alors avoir

$$S_a^\gamma S_b^\delta \ldots C_\mu = S_c^\varepsilon S_d^\eta \ldots C_\gamma,$$

il faudrait qu'une substitution C qui n'échange que des lettres pût s'exprimer à l'aide d'un produit de substitutions S qui n'échangent que des indices. Cela étant impossible, les $p^{q+\beta}$ substitutions considérées sont toutes distinctes; elles forment un groupe, car le produit de deux d'entre elles peut être ramené à la même forme en faisant reculer leur facteur C; ce produit appartient donc à l'ensemble des $p^{q+\beta}$ substitutions.

Il reste à trouver la puissance la plus élevée de p contenue dans $(pq+r)!$; si l'on met à part les facteurs non divisibles par p on trouve $p^q q!$ et p^β étant la plus haute puissance contenue dans $q!$, $p^{\beta+q}$ est la plus haute puissance de p contenue dans $(pq+r)!$. Il est donc prouvé que l'on peut trouver un groupe d'ordre $p^{\beta+q}$ où $p^{\beta+q}$ est la plus haute puissance de p contenue dans $k!$, où k est le nombre des lettres.

167. *Si le groupe* G *d'ordre* g *contient les groupes* H, K *d'ordres* h, k *et si* H *ne contient pas de substitutions (autre que* 1) *semblables à celles de* K, *on a* $g =$ *multiple de* hk.

En effet, appelons S les substitutions de H, T celles de K et U celles de G, il existe hk substitutions de G de la forme

$$S_\alpha U_1 T_\beta,$$

toutes différentes, car si l'on avait

$$S_\alpha U_1 T_\beta = S_{\alpha_1} U_1 T_{\beta_1},$$

on en déduirait

$$U_1 T_\beta T_{\beta_1}^{-1} U_1^{-1} = S_\alpha^{-1} S_{\alpha_1},$$

ce qui est absurde, puisque $T_p T_{\beta_1}^{-1}$ et $S_\alpha^{-1} S_{\alpha_1}$ ne peuvent être toutes deux égales à 1 et ne sont pas semblables.

Soit alors U_2 une substitution non comprise parmi les hk

substitutions considérées; G contiendra encore hk substitutions distinctes de la forme

$$S_\alpha U_2 T_\beta,$$

distinctes des précédentes; car, si l'on avait

$$S_\alpha U_1 T_\beta = S_{\alpha_1} U_2 T_{\beta_1},$$

U_2 se trouverait parmi les substitutions déjà considérées. Si l'on continue de cette manière, on épuise toutes les substitutions de G à savoir hk substitutions dans chaque série, et il faut que hk divise g.

168. *Tout groupe* G *dont l'ordre est divisible par un nombre premier p contient une substitution d'ordre p.*

Supposons que le groupe G soit formé avec k lettres et que son ordre soit égal à g, ce groupe et le groupe Γ considéré § 166, supposé d'ordre p^β, sont contenus dans le groupe général d'ordre $k!$. Si G ne contenait pas de substitution d'ordre p, il ne contiendrait pas de substitution semblable à celles de Γ; car Γ ne contient que des substitutions dont l'ordre est une puissance de p (159), et il y a toujours des puissances des substitutions semblables à celles-ci dont l'ordre est p; $k!$ devrait donc être divisible par gp^β (167), ce qui est impossible si g est divisible par le facteur premier p, puisque p^β est la puissance la plus élevée de p contenue dans $k!$. G doit donc contenir au moins une substitution d'ordre p.

Groupes transitifs et intransitifs.

169. Un groupe est dit *transitif*, si au moyen de ses substitutions on peut amener une quelconque des lettres à la place occupée par chacune des autres; il est *intransitif* dans le cas contraire.

Quand un groupe est intransitif, une lettre a_1 peut remplacer $a_2, a_3, \ldots, a_p$, mais non $b_1, b_2, \ldots, b_q$, alors une lettre a ne peut remplacer une lettre b; sans quoi, en combinant deux substitutions du groupe a, on pourrait faire occuper à a_1 la place d'une lettre b.

Ainsi, dans un groupe intransitif, on pourra distribuer les lettres en deux ou plusieurs systèmes tels que dans un même système les lettres ne puissent que s'échanger entre elles, et non avec celles des autres systèmes; toute substitution du groupe se décomposera en cycles qui ne contiennent que des lettres d'un même système.

Naturellement, il faut dire quelles sont les lettres en question. Ainsi le groupe général de $n-1$ lettres est transitif si l'on n'a à considérer que les $n-1$ lettres de ce groupe; il devient intransitif par rapport à un système contenant, outre ces $n-1$ lettres, d'autres lettres que le groupe considéré ne déplace pas.

Un groupe est m fois transitif s'il est possible de faire passer, au moyen de ses substitutions, à la fois m lettres données à la place de m autres lettres arbitraires distinctes ou non des premières.

On voit facilement que, si l'on peut remplacer m lettres quelconques par m lettres données, on peut également remplacer m lettres quelconques par m lettres quelconques.

Le groupe général de n lettres est $n-1$ fois transitif, le groupe alterné $n-2$ fois. Si un groupe de n lettres contient une substitution circulaire de n lettres, il est au moins une fois transitif; s'il contient en outre une substitution circulaire de $n-1$ lettres, il est deux fois transitif, etc.

176. *Si l'on considère des lettres déterminées $a, b, c, \ldots$ d'un groupe* G (*transitif ou intransitif*) *et si le groupe* H *qui ne déplace pas ces lettres est d'ordre k,* G *est d'ordre kp, p désignant le nombre des systèmes de places que prendront $a, b, c, \ldots$ par les substitutions de* G.

Soient, en effet,

$$1, \quad T_1, \quad T_2, \quad \ldots, \quad T_{k-1}$$

les substitutions de H, et R une des autres substitutions; les substitutions

$$R, \quad T_1 R, \quad T_2 R, \quad \ldots, \quad T_{k-1} R$$

transportent toutes les lettres $a, b, c, \ldots$ aux mêmes places, et cette propriété n'appartient qu'à ces substitutions, car, si une autre substitution R_1 possédait cette propriété, $R_1 R^{-1}$ laisserait les lettres invariables et appartiendrait au groupe des substitutions T. R_1 se trouverait alors donc dans la suite TR. Les substitutions de G peuvent donc se partager en p séries de k substitutions.

Si G *est m fois transitif*, si l'on considère m lettres a, b, c, ..., le nombre total des lettres étant n, on aura

$$p = n(n-1)\ldots(n-m+1),$$

d'où l'on voit que l'*ordre d'un groupe m fois transitif de n lettres est divisible par* $n(n-1)\ldots(n-m+1)$.

Si G est intransitif et si l'on considère α lettres, échangeables entre elles, les substitutions qui n'échangent pas ces α lettres forment un groupe; soit k son ordre; le nombre des systèmes de places auxquelles on peut amener ces lettres est un diviseur de $\alpha!$; l'ordre de G est donc un diviseur de $k\alpha!$; si l'on raisonne de la même façon sur les $n-\alpha$ lettres restantes et ainsi de suite, on voit que l'ordre de G est un diviseur de $\alpha!\,\beta!\,\gamma!\ldots$, où α, β, γ, ... satisfont à la relation

$$\alpha + \beta + \gamma \ldots = n$$

et désignent le nombre de lettres des systèmes dont les lettres peuvent être échangées.

171. *Si un groupe est m fois transitif, et s'il contient une substitution qui ne déplace pas plus de m lettres, il est le groupe général ou le groupe alterné.*

Soit S une substitution qui déplace au plus m lettres; soit S_1 une substitution quelconque semblable à S; le groupe doit contenir une substitution qui change les lettres de S dans les lettres correspondantes de S_1 (169); si l'on transforme S par cette substitution, on obtient S_1; cette substitution entrera donc aussi dans le groupe. Soit

$$(a_1 a_2 \ldots a_p)$$

un cycle de S. Pour S_1 on peut prendre une substitution contenant le cycle

$$(a_p a_{p-1} \ldots a_4 a_2 a_3 a_1),$$

les autres cycles de S et S_1 étant les mêmes, à l'ordre des lettres près qui sera renversé. G renferme aussi la substitution

$$S_1 S = (a_1 a_3 a_2),$$

et par suite toutes les substitutions circulaires du troisième ordre ; G contient donc le groupe alterné (**164**).

Cette démonstration suppose que S contient un cycle de trois lettres au moins. Dans le cas contraire on peut prendre pour les deux cycles de S et S_1

$$(a_1 a_2) \quad \text{et} \quad (a_2 a_3),$$

a_3 étant une lettre qui n'entre pas dans S; alors

$$SS_1 = (a_1 a_2 a_3).$$

172. *Quand un groupe m fois transitif contient une substitution qui ne déplace pas plus de* $2m-4$ *lettres, il est le groupe alterné ou le groupe général.*

Soit, en effet,

$$S = (abc\ldots)(def\ldots)(g\ldots)$$

une des substitutions qui déplace q lettres, et supposons $m < q < 2m-3$. Le groupe contient une substitution T qui ne déplace pas $m-1$ de ces lettres $a, b, c, \ldots, d, e,$ et qui remplace les autres par $\alpha, \beta, \gamma, \ldots,$ dont l'une au moins, α, qui remplace f, n'existe pas parmi les q lettres considérées. Le groupe contient alors la substitution

$$U = TST^{-1} = (abc\ldots)(de\alpha\ldots)(\beta\ldots)\ldots,$$

et la substitution $S^{-1}U$, qui ne contient que les lettres $e, \alpha, \beta, f, g, \ldots,$ et qui ne peut être 1, puisqu'elle déplace au moins α; le nombre de ses lettres est au plus

$$2(q-m+1)+1 = 2q-2m+3 < q;$$

de cette manière, à l'aide de la substitution donnée, on peut

en trouver une autre déplaçant moins de lettres et, en continuant ainsi, on finit par en trouver une qui déplace au plus m lettres, ce qui démontre le théorème.

Le nombre minimum des lettres déplacées par une substitution d'un groupe est ce que l'on appelle la *classe* du groupe.

173. *L'ordre d'un groupe de n lettres, m fois transitif, qui ne contient pas le groupe alterné, est un diviseur de*

$$\frac{n!}{\alpha!},$$

α désignant le plus grand des nombres m et $2m-4$.

En effet, si l'on forme le groupe général de α lettres, il ne contient pas de substitution semblable à une substitution du groupe donné déplaçant plus de α lettres; si l'ordre du groupe donné est g, $g\alpha!$ sera un diviseur de $n!$ (167).

174. *Un groupe de degré n, qui ne contient pas le groupe alterné, ne peut pas être plus de q fois transitif, q désignant le plus petit des nombres*

$$\frac{n+4}{3}, \quad \frac{n}{2}.$$

Si le groupe est q fois transitif, son ordre (170) est un multiple de

$$n(n-1)\ldots(n-q+1);$$

ce nombre doit (173) être un diviseur de $\frac{n!}{\alpha!}$, ou $(n-q)!$ doit être divisible par $\alpha!$; on doit donc avoir

$$n-q \geqq \alpha, \qquad q \leqq n-\alpha,$$

où α est le plus grand des nombres q, $2q-4$; il en résulte

$$q \leqq \frac{n}{2} \qquad \text{et} \qquad q \leqq \frac{n+4}{3}.$$

M. Jordan a fait voir qu'un groupe de degré $p+\alpha$ ne peut

être plus de α fois transitif, si p est premier et si $\alpha > 2$ (*Bulletin de la Soc. math. de France*, t. I).

175. *Si un groupe* G, *n fois transitif, contient un groupe* H, *permutable avec toutes les substitutions de* G, H *est au moins* $n-1$ *fois transitif.* (Ce théorème est soumis à une exception.)

Le théorème est vrai pour $n=2$, car, si l'on désigne par $S=(ab\ldots)(\ldots)\ldots$ une substitution de H, G contiendra une substitution T qui remplace a, b par deux lettres arbitraires. H contiendra alors TST^{-1}, qui remplace une lettre arbitraire par une lettre arbitraire.

A l'aide de G et de H, formons deux nouveaux groupes G_1, H_1, en laissant de côté les substitutions qui contiennent une lettre déterminée, a par exemple; H_1 est contenu dans G_1, il est permutable avec toutes les substitutions de G_1. Comme G est n fois transitif, G_1 l'est $n-1$ fois.

H est une fois de plus transitif que H_1, car, au moyen des substitutions qui ont été écartées, on peut placer a où l'on veut; le théorème énoncé a donc lieu pour G et H; s'il a lieu pour G_1 et H_1, et comme il a été démontré pour le cas où $n=2$, il est général, pourvu toutefois que l'un des groupes H_1 ne se compose pas de la seule substitution identique 1.

Il y a donc lieu de considérer à part le cas où $H_1=(1)$; dans ce cas, toutes les substitutions de H (à part la substitution 1) contiennent toutes les lettres qui entrent dans G, sans quoi on pourrait prendre pour a une des lettres qui font défaut; une seule substitution de H peut remplacer a par b. Soient, en effet, T et U deux substitutions différentes; remplaçant a par b, TU^{-1} est différent de 1 et ne peut contenir a; d'un autre côté, a s'échange avec toutes les autres lettres, le nombre des substitutions est alors égal à celui des lettres; il en résulte que H est une fois transitif (170).

Si G est deux fois transitif, le théorème est vrai; on n'a donc à considérer que le seul cas $n>2$. Si H contenait une substitution

$$S=(abc\ldots)(\ldots),$$

il contiendrait une autre substitution remplaçant a par b

$$S_1 = (abd\ldots)(\ldots),$$

car si G est plus de deux fois transitif, il existe une substitution qui transforme S en S_1. On voit donc que les cycles de H ne contiennent que deux lettres, et l'on en conclut facilement que l'on ne peut avoir que $n = 3$.

Puisque les substitutions de H sont du second ordre, l'ordre de H est une puissance de 2. Les substitutions de H sont échangeables, car si S et T sont deux de ces substitutions, on a

$$(ST)(ST) = 1, \qquad \text{d'où} \qquad ST = TS.$$

Le groupe

$$1, \quad (ab)(cd), \quad (ac)(bd), \quad (ad)(bc),$$

contenu dans le groupe général du quatrième ordre, est un exemple.

Sur les groupes transitifs qui contiennent d'autres groupes également transitifs.

176. Soit G un groupe transitif de degré supérieur à p qui contient un groupe m fois transitif, A, permutant les lettres a_1, a_2, ..., a_p. Les substitutions de G, qui ne permutent que ces lettres, forment un groupe qui contient A et qui est au moins m fois transitif, nous supposerons que ce groupe soit A.

Soient b_1, b_2, ... les autres lettres permutées par G; supposons que G contienne un groupe renfermant A et permutant les lettres $a_1, a_2, \ldots, a_p, b_1$. Ce groupe doit contenir des substitutions qui remplacent b_1 par un a et, par suite, des substitutions remplaçant b_1 par un a quelconque. Une pareille substitution permet de mettre b_1 à une place quelconque; au moyen des substitutions A, on peut mettre m des lettres a à des places quelconques; le groupe est donc au moins $m + 1$ fois transitif.

Ce groupe peut lui-même être contenu dans un autre groupe contenu dans G, lequel déplace les lettres $a_1, a_2, \ldots, a_p, b_1, b_2$

et est au moins $m + 2$ fois transitif. En continuant ainsi, deux cas pourront se présenter :

1° Après avoir ajouté q lettres une à une, nous parvenons au groupe G au moins $m + q$ fois transitif;

2° Nous arrivons à un groupe que nous ne pouvons plus généraliser de cette manière, parce qu'il n'existe plus de sous-groupe contenant une lettre de plus; nous désignerons maintenant par A ce groupe m fois transitif, permutant les p lettres $a_1, a_2, \ldots, a_p$. G contient au moins deux lettres b, et de telle sorte qu'aucune de ses substitutions ne contienne pas seulement une seule lettre b; car s'il contenait une semblable substitution, il existerait un sous-groupe échangeant seulement les a et un b, ce qui est contraire à notre hypothèse.

Considérons maintenant, parmi les substitutions qui échangent un a avec un b, sans changer tous les a avec des b, une substitution dans laquelle les b sont en nombre minimum; soit T cette substitution, supposons qu'elle remplace a_1 par b_1, a_1 ne remplaçant pas lui-même un b; nous supposerons qu'elle remplace un b par un autre b, qu'elle remplace, par exemple, b_r par b_s; on aura

$$T = \begin{pmatrix} b_1 & b_s & a_1 & \ldots \\ a_1 & b_r & a_r & \ldots \end{pmatrix}.$$

Dans le groupe A, il entre une substitution S qui échange a_1 en a_r; si on la transforme par T, on obtient une substitution qui remplace b_1 par un a, dans laquelle b_s n'entre pas et qui, en outre, ne contient pas d'autres b que ceux qui entrent dans T. La substitution inverse remplace un a par un b et ne contient pas b_s. Or cela est contraire à notre hypothèse. On a donc le théorème suivant :

Une substitution qui remplace un a par un b et qui contient le minimum de lettres b doit remplacer chaque a par un b, ou ne doit remplacer aucun b par un autre b.

Dans le premier cas, le nombre des lettres b doit être au moins égal au nombre des lettres a.

Dans le second cas, on a

$$T = \begin{pmatrix} b_1 & b_2 & \dots \\ a_1 & a_2 & \dots \end{pmatrix}.$$

Nous supposerons maintenant A *au moins deux fois transitif*. Si nous supposons que chaque a n'est pas remplacé par un b, a_r par exemple sera remplacé par a_s, où r pourra être égal à s. A contient une substitution qui ne déplace pas a_1 et qui remplace a_r par a_2. Si on la transforme par T, on obtient une substitution qui ne contient pas b_1 et qui remplace a_s par b_2; or cela est impossible, T doit donc remplacer tout a par un b. Donc :

Si A *est deux fois transitif, une substitution* T, *qui remplace un a par un b, doit remplacer chaque a par un b.*

Nous désignerons par $b_1, b_2, \dots, b_p$ les b qui, dans T, remplacent les a; s'il y a plus de p lettres b, nous les désignerons par c. En transformant A par T, on obtient un groupe B des lettres b, m fois transitif.

Il existe une substitution qui remplace a_1 par c_1; elle remplace, comme on l'a vu, tous les a par des b ou des c; si parmi les lettres substituées aux a il se trouve des b, transformons cette substitution par T^{-1}, nous obtiendrons une substitution qui remplacera les a en partie par des a, en partie par des c; or cela est impossible; donc toute substitution remplaçant un a par un c doit remplacer chaque a par un c, il y a donc au moins p lettres c; on prouve aisément, comme plus haut, qu'une substitution qui remplace un b par un c remplace chaque b par un c.

Si l'on continue ainsi, on voit que les lettres de G peuvent être réparties en systèmes de p lettres $a, b, c, \dots,$ avec les indices $1, 2, 3, \dots, p$; les substitutions du groupe échangent, soit les lettres d'un même système, soit toutes les lettres d'un système avec toutes les lettres d'un autre système.

Les groupes qui jouissent de cette propriété sont dits *imprimitifs*. Les autres groupes sont dits *primitifs*. Les groupes imprimitifs sont une seule fois transitifs, car ils ne peuvent, par exemple, remplacer à la fois a_1 par a_2 et a_2 par b_1.

177. On a supposé le groupe A au moins deux fois transitif; s'il était seulement une fois transitif, la substitution T, qui contient le plus petit nombre de lettres b peut échanger les lettres a en partie par des lettres a, en partie par des lettres b.

Nous désignerons les a, qui sont remplacés par des b, par $a_1, a_2, \ldots$; les autres seront désignés par α. On a alors

$$T = \begin{pmatrix} b_1 & b_2 & \ldots & \alpha_2 & \ldots \\ a_1 & a_2 & \ldots & \alpha_1 & \ldots \end{pmatrix}$$

où α_2 pourra être un a.

A contient une substitution S_1 qui remplace a_1 par a_2; supposons qu'elle remplace un a par un α; transformons cette substitution par T, on obtient une substitution dont l'inverse remplace un α par un b et b_2 par b_1; or c'est impossible : donc toute substitution de A, qui remplace un a par un α, remplace tout a par un α; nous pouvons continuer ce raisonnement comme plus haut et montrer que A est imprimitif. On peut donc énoncer le théorème suivant :

Un groupe transitif de $p+q$ lettres, qui contient un groupe de p lettres qui est m fois transitif, et qui ne contient pas de groupe imprimitif de p lettres, est imprimitif ou au moins $m+q$ fois transitif.

Deux cas particuliers sont à remarquer.

Un groupe transitif du degré n qui contient une substitution circulaire d'ordre p, p désignant un nombre premier $> \frac{1}{2}n$, est au moins $(n-p+1)$ transitif.

La substitution circulaire et ses puissances forment un groupe d'ordre p qui ne peut être imprimitif, et ni p, ni aucun nombre plus grand que p et plus petit que n ne peut diviser n, de sorte que le groupe considéré ne peut être imprimitif.

Un groupe transitif qui contient un sous-groupe alterné est imprimitif ou contient le groupe alterné formé avec toutes les lettres.

Car un groupe de degré n ne peut être au moins $n-2$ fois transitif que dans le cas où il est le groupe alterné ou le groupe général.

178. *Ordre des groupes imprimitifs.* — Dans un groupe G imprimitif d'ordre mp les substitutions des lettres $a_1, a_2, \ldots, a_p$; $b_1, b_2, \ldots, b_p$; $c_1, c_2, \ldots, c_p$; ... ne peuvent remplacer que des lettres d'un même système par des lettres d'un même système. Soient T_1 et T'_1 deux substitutions qui permutent les lettres de la même manière, abstraction faite des indices, et $S_1, S_2, \ldots$ les substitutions qui n'opèrent que sur les indices. La substitution $T'_1 T_1^{-1}$ appartient alors à la série des substitutions S; dans la suite

$$T_1, \quad S_1 T_1, \quad S_2 T_1, \quad \ldots$$

se trouvent toutes les substitutions de G qui, sans avoir égard aux indices, échangent les mêmes lettres de la même façon. Soit

$$U_1 = (abc\ldots)(de\ldots)$$

une substitution dont les lettres sont échangées de la même façon.

A l'aide d'une autre substitution de G, qui n'appartient ni à la série S, ni à la série ST_1, formons la série

$$T_2, \quad S_1 T_2, \quad S_2 T_2, \quad \ldots,$$

caractérisée par la substitution U_2 et ainsi de suite.

Les substitutions U forment un groupe, car si $T_\alpha T_\beta$ entre dans la suite qui commence par T_γ, on a

$$U_\alpha U_\beta = U_\gamma.$$

L'ordre de G est donc un diviseur de

$$m!(p!)^m,$$

car G est contenu dans le groupe imprimitif pour lequel le groupe U est le groupe général d'ordre $m!$ et $S_1, S_2, \ldots$ et leurs produits sont donnés par les groupes généraux que l'on peut former avec les m systèmes de lettres.

Un groupe H est *isomorphe* avec un groupe K, quand à chaque substitution de K correspond une substitution de H et à chaque substitution de H une ou plusieurs substitutions de K, le produit de deux substitutions de K correspondant au produit des substitutions correspondantes de H.

De cette définition et de ce qui précède, il résulte que le groupe U est isomorphe avec G.

Exemple. — Si l'on prend

$$U_1 = 1, \quad U_2 = (ab), \quad p = 2,$$

on peut former le groupe du quatrième degré et du huitième ordre

$$1, \quad (a_1 a_2), \quad (b_1 b_2), \quad (a_1 a_2)(b_1 b_2),$$
$$(a_1 b_1 a_2 b_2), \quad (a_1 b_1)(a_2 b_2), \quad (a_1 b_2)(a_2 b_1), \quad (a_1 b_2 a_2 b_1);$$

ce groupe est imprimitif et isomorphe avec 1, (ab).

Groupe d'une fonction et nombre des valeurs qu'elle peut acquérir.

179. *Les substitutions que l'on peut faire subir aux lettres dont dépend une fonction, sans altérer la valeur de cette fonction, forment un groupe.*

En effet, si une fonction reste inaltérée quand on opère avec la substitution S ou avec la substitution T, il est clair qu'elle ne changera pas non plus quand on effectuera la substitution ST; celle-ci fait donc partie des substitutions qui n'altèrent pas la fonction, qui par suite forment un groupe. Ce groupe s'appelle le *groupe de la fonction* et l'on dit que la fonction *admet* les substitutions du groupe. Si la fonction par exemple est symétrique, son groupe sera le groupe général; si elle est alternée, son groupe sera le groupe alterné. Le groupe du huitième ordre et du quatrième degré considéré (178) appartient aux fonctions (a_1 est remplacé par x_1, etc., ...)

$$(x_1 + x_2)(x_3 + x_4), \quad x_1 x_2 + x_3 x_4, \quad (x_1 - x_2 + x_3 - x_4)^2, \quad \ldots.$$

Soit maintenant g l'ordre d'un groupe d'une fonction, qui se

compose des substitutions

$$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{g-1}.$$

Le groupe général, si le nombre des lettres est n, pourra être représenté par les $\frac{n!}{g}$ séries de substitutions

$$T_\alpha, \quad T_\alpha S_1, \quad T_\alpha S_2, \quad \ldots, \quad T_\alpha S_{g-1},$$

et comme les substitutions S ne changent pas la fonction considérée, toutes les substitutions de la série feront acquérir à la fonction la même valeur que T_α.

On obtient donc le nombre des valeurs distinctes que peut acquérir une fonction de n lettres en divisant $n!$ par l'ordre du groupe de la fonction.

Exemple. — Les trois valeurs

$$x_1 x_2 + x_3 x_4, \quad x_1 x_3 + x_2 x_4, \quad x_1 x_4 + x_2 x_3$$

pourront se déduire de la première au moyen des substitutions

$$1, \quad (x_2 x_3), \quad (x_2 x_4).$$

Le groupe de la fonction se compose de huit substitutions; si on les multiplie par les trois précédentes, on obtient les vingt-quatre substitutions du groupe général. La somme et le produit des trois fonctions considérées ne sont altérés par aucune des vingt-quatre substitutions en question, elles sont symétriques.

180. On peut toujours former une fonction admettant un groupe donné; on peut, par exemple, former une fonction y dont toutes les valeurs sont distinctes;

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \ldots$$

où $\alpha_1, \alpha_2, \ldots$ sont des nombres différents, est dans ce cas; si l'on désigne par $y_1, y_2, \ldots$ les valeurs que prend y par les substitutions du groupe donné

$$z = (z - y_1)(z - y_2)\ldots,$$

où α est indéterminé, est inaltérée par les substitutions du groupe et variable pour toute autre substitution.

181. *Si le groupe de la fonction y_0 est* G *et si la substitution* T *transforme y_0 en y_1, le groupe transformé de* G *par* T *appartiendra à y*.

Soit, en effet, S une substitution de G. S ne change pas y_0; TST^{-1} ne changera pas y_1; car on a

$$Ty_0 = y_1 \qquad \text{ou} \qquad T^{-1}y_1 = y_0;$$

ainsi

$$TST^{-1}y_1 = TSy_0 = Ty_0 = y_1.$$

Lorsque G est permutable avec T, le groupe transformé coïncide avec G, de sorte que le groupe appartient aussi à y_1. On voit ainsi que *si le groupe* G *appartient à y_0, il appartient aussi aux fonctions transformées de y_0 par les substitutions permutables avec* G.

Indice d'un groupe.

182. On appelle *indice* d'un groupe, le quotient obtenu en divisant l'ordre du groupe général par l'ordre de ce groupe.

Considérons une fonction qui ne soit pas altérée par toutes les substitutions d'un groupe, mais qui soit altérée par toutes les autres, le nombre des valeurs distinctes de cette fonction, d'après ce que l'on a vu (179), sera égal à l'indice du groupe. L'indice du groupe général est 1, celui du groupe alterné est 2.

On a vu (170) que l'ordre d'un groupe intransitif de n lettres était un diviseur de $\alpha!\beta!\ldots$ où $\alpha+\beta+\ldots=n$. L'indice de ce groupe est alors un multiple de

$$\frac{n!}{\alpha!\beta!\ldots}.$$

L'ordre d'un groupe imprimitif est (178) un diviseur de

$$m!(p!)^m,$$

quand le groupe contient m systèmes de p lettres. La plus petite valeur que puisse prendre l'indice i est donc

$$i = \frac{mp(mp-1)\ldots(m+1)}{2.3\ldots p.2.3\ldots p\ldots 2.3.p},$$

le numérateur et le dénominateur contenant le même nombre de facteurs. Pour $n=4$, on obtient le groupe de l'exemple 178 dont l'indice est 3. Pour $n=6$, le plus petit indice est 10, pour $n=8$ il est 35 et il croît rapidement. On peut prouver que cet indice pour $n>4$ est supérieur à n, bien que ce fait soit presque évident.

183. Nous allons encore considérer un groupe primitif qui ne contient pas de groupe alterné. Soient $p_1, p_2, \ldots$ des nombres premiers distincts dont la somme ne soit supérieure au nombre n des lettres; avec p_1 lettres formons une substitution circulaire non contenue dans le groupe; les substitutions circulaires de p_2 des lettres restantes ne pourront pas toutes entrer dans le groupe; prenons une de celles qui n'y entrent pas et continuons de cette façon autant que possible; soit T la substitution d'ordre $p_1 p_2 \ldots$ obtenue en faisant le produit de ces substitutions circulaires.

Le groupe ne peut contenir ni T ni ses puissances, car parmi les puissances d'une telle substitution se trouve au moins une des substitutions circulaires qui n'entrent pas dans le groupe.

Soient alors $1, S_1, S_2, \ldots$ les substitutions du groupe considéré, q leur nombre; formons toutes les substitutions telles que $T^\alpha S_\beta$; elles sont toutes différentes et leur nombre est $qp_1p_2\ldots$: ce nombre est au plus égal à $n!$; donc

$$q \leqq \frac{n!}{p_1 p_2 \ldots}; \quad i = \geqq p_1 p_2 \ldots$$

Il en résulte que l'*indice du groupe ne peut être inférieur au produit des nombres premiers dont la somme ne dépasse pas n.*

184. Supposons que les nombres premiers employés soient $p_1, p_2, \ldots, p_\alpha$; alors

$$p_1 + p_2 + \ldots + p_\alpha \leqq n,$$

mais p_β désignant un nouveau nombre premier quelconque

$$p_1+p_2+\ldots+p_\alpha+p_\beta>n,$$

le nombre

$$p_1p_2\ldots p_{\alpha-1}-p_\alpha,$$

p_α désignant le plus grand de ces nombres premiers ou celui qui en approche le plus n'est pas divisible par un des nombres p_1, p_2, ..., p_α; c'est donc un nombre premier ou un produit de nombres premiers différents de ceux-ci : p_β peut donc être pris inférieur ou égal à ce produit; alors

$$p_1+p_2+\ldots+p_{\alpha-1}+p_1p_2\ldots p_{\alpha-1}>n$$

ou

$$i\geqq p_1p_2\ldots p_{\alpha-1}p_\alpha>\frac{1}{2}p_\alpha n.$$

De cette manière, on voit qu'il n'existe qu'un seul groupe d'indice plus grand que 2 et moindre que n, à savoir pour $n=4$. Parmi les groupes de n lettres dont l'indice est n se trouve le groupe général de $n-1$ lettres. Ce groupe appartient aux fonctions de n lettres symétriques par rapport à $n-1$ d'entre elles. Si l'on prend pour les nombres premiers p_1, p_2, ..., les nombres 2, 3, 5, ..., on voit qu'un groupe d'indice n n'est possible que pour

$$n<10(=2+3+5);$$

et comme

$$9=7+2,\qquad 8=3+5,\qquad 7=2+5,\qquad 5=2+3,$$

il reste à considérer les cas où $n=4$ et $n=6$. On voit facilement que, pour $n=4$, il n'y a pas de groupe transitif d'indice 4; pour $n=6$, il y a un groupe d'indice 6 trois fois transitif appartenant aux fonctions de six lettres possédant six valeurs sans être symétriques par rapport à cinq d'entre elles; on obtient une pareille fonction en multipliant entre elles les expressions

$$ab+cd+ef,\quad ac+be+fd,\quad ad+bf+ce,$$
$$ae+bd+fc,\quad af+bc+ed.$$

Il est donc impossible de trouver une fonction de n lettres possédant plus de deux et moins de n valeurs, excepté si $n=4$. Il est impossible de trouver une fonction de n lettres ayant n valeurs, si elle n'est pas symétrique par rapport à $n-1$ lettres, excepté pour $n=6$.

Des substitutions linéaires.

185. Considérons une substitution formée avec les lettres $a_0, a_1, \ldots, a_{n-1}$; si, dans une transformation d'indices, l'un d'eux devenait supérieur à $n-1$, il faudrait sous-entendre qu'il doit être remplacé par le reste de sa division par n; α, $n+\alpha$, $2n+\alpha$, ... seront donc considérés comme représentant le même indice. Représentons par le symbole

$$\binom{F(z)}{z}$$

la substitution qui remplace la lettre qui porte l'indice z en général par une autre portant l'indice $F(z)$. La fonction $F(z)$ devra être telle que, pour $z=0, 1, 2, \ldots, n-1$, elle prenne à l'ordre près ces mêmes valeurs.

Nous considérerons en particulier les substitutions *linéaires*

$$\binom{az+b}{z};$$

$F(z)=az+b$ remplira la condition dont nous venons de parler, si b désigne un nombre entier quelconque et si a est un nombre premier avec n, car on obtient des restes tous différents en divisant $az+b$ par n et en attribuant à z les valeurs $0, 1, 2, \ldots, n-1$.

Les substitutions circulaires sont un cas particulier des substitutions linéaires; par exemple, si

$$S=(a_0 a_1 a_2 \ldots a_{n-1}),$$

$$S=\binom{z+1}{z}, \qquad S^2=\binom{z+2}{z}, \qquad S^3=\binom{z+3}{z}, \qquad \ldots,$$

$$\binom{2z}{z}=(a_1 a_2 a_4 a_8 \ldots), \qquad \binom{2z+1}{z}=(a_0 a_1 a_3 a_7 \ldots), \qquad \ldots.$$

Le nombre des substitutions linéaires de n lettres est $n\varphi(n)$, $\varphi(n)$ désignant le nombre des entiers premiers avec n et inférieurs à n; a peut, en effet, recevoir $\varphi(n)$ valeurs et b peut en recevoir n. Les substitutions linéaires forment un groupe, car

$$\begin{pmatrix} cz+d \\ z \end{pmatrix}\begin{pmatrix} az+b \\ z \end{pmatrix} = \begin{pmatrix} acz+ad+b \\ z \end{pmatrix}.$$

Ce groupe est celui qui a été considéré (162), car si l'on transforme

$$(a_0 a_1 a_2 \ldots)$$

par

$$\begin{pmatrix} az+b \\ z \end{pmatrix},$$

on obtient une substitution dans laquelle la série des indices est

$$b, \quad a+b, \quad 2a+b, \quad \ldots,$$

la substitution considérée est donc transformée en sa puissance a.

D'après ce qui précède, on voit que toutes les substitutions du groupe linéaire peuvent s'obtenir en combinant par multiplication deux substitutions

$$\begin{pmatrix} z+1 \\ z \end{pmatrix}, \quad \begin{pmatrix} az \\ z \end{pmatrix},$$

où a est racine primitive de $x^{\varphi(n)} \equiv 1$.

186. *Si n est égal à un nombre premier p, l'ordre du groupe linéaire est $p(p-1)$, et il n'y a pas d'autre groupe de p lettres qui soit du même ordre.*

En vertu du théorème de Cauchy (168), un groupe d'ordre $p(p-1)$ doit contenir une substitution circulaire d'ordre p; soient

$$1, \quad S, \quad S^2, \quad \ldots, \quad S^{p-1}$$

les puissances successives de cette substitution et T une autre substitution du groupe; toutes les substitutions de la forme

$$S^\alpha T S^\beta$$

ne peuvent être différentes, car leur nombre est p^2; on doit donc avoir, pour des valeurs convenables des exposants,

$$S^\alpha T S^\beta = S^\gamma T S^\delta$$

ou

$$T S^{\beta-\delta} T^{-1} = S^{\gamma-\alpha};$$

d'où l'on tire, en élevant les deux membres à une puissance convenable,

$$T S T^{-1} = S^m.$$

T transforme donc les substitutions S en leurs puissances, et ces substitutions forment, comme on l'a vu, le groupe linéaire.

187. La notion de substitution linéaire est susceptible d'extension, et l'on peut concevoir des fonctions linéaires fractionnaires en posant

$$F(z) = \frac{az + b}{a_1 z + b_1}.$$

Lorsque $F(z) = q$, il faut supposer que q est donné par l'équation indéterminée

$$az + b = q(a_1 z + b_1) + py$$

(on suppose n égal à un nombre premier p). Si une valeur de z rend le dénominateur $a_1 z + b_1$ multiple de p, on a $q = \infty$, une lettre devra alors porter l'indice ∞, et on a les $p+1$ lettres

$$a_0, \quad a_1, \quad \ldots, \quad a_{p-1}, \quad a_\infty.$$

La lettre qui porte l'indice ∞ sera remplacée par celle qui porte l'indice α donné par la formule

$$\alpha = \frac{a}{a_1} \qquad \text{ou} \qquad a_1 \alpha + py = a.$$

Ces substitutions forment un groupe d'ordre $(p-1)p(p+1)$. Nous n'en dirons pas davantage sur ce sujet.

On a étendu ces notions en considérant des lettres avec

plusieurs indices, par exemple x et y. Ainsi le symbole

$$\begin{pmatrix} x, & ax + by \\ y, & a_1 x + b_1 y \end{pmatrix}$$

ou

$$\begin{pmatrix} ax + by, & a_1 x + b_1 y \\ x & y \end{pmatrix}$$

représente une substitution qui remplace x et y par $ax + by$, $a_1 x + b_1 y$; comme plus haut, les indices doivent être censés remplacés par le reste de leur division par un nombre donné. Ces considérations trouvent leur application quand le nombre des lettres est la puissance d'un nombre premier. Quand le nombre donné (module) est p, a_{xyz} représente un ensemble de p^3 lettres.

Ordinairement, on appelle *groupe linéaire* le groupe général d'ordre $n\varphi(n)$ dont nous avons parlé; mais on comprend aussi sous cette dénomination d'autres groupes contenus dans ce groupe et transitifs; leurs ordres sont de la forme αn, α désignant un diviseur de $\varphi(n)$.

CHAPITRE III.

THÉORIE DE GALOIS.

Groupe d'une équation.

188. Une équation irréductible peut devenir réductible si l'on suppose certaines irrationnelles données et pouvant entrer dans les coefficients. Ainsi, par exemple, l'équation

$$x^2 - 4x + 1 = 0$$

est irréductible, mais elle devient réductible si l'on se permet d'employer l'irrationnelle $\sqrt{3}$; elle se réduit alors aux équations

$$x - 2 + \sqrt{3} = 0 \quad \text{et} \quad x - 2 - \sqrt{3} = 0;$$

quand on se permet ainsi d'employer dans les calculs certaines expressions, on dit que ces expressions sont *adjointes*. L'équation considérée est réductible quand on adjoint $\sqrt{3}$; elle reste irréductible quand on adjoint $\sqrt{5}$, $\sqrt{7}$, ... Toute équation devient réductible en adjoignant une ou plusieurs de ses racines.

Dans la suite, nous supposerons l'adjonction de certaines irrationnelles, et ces irrationnelles pourront alors entrer, sous forme rationnelle, dans les coefficients des équations que nous aurons à considérer.

Galois a montré qu'à toute équation correspondait un certain groupe de substitutions servant à la caractériser, ou plus exactement, servant à caractériser une classe d'équations. Quand on connaît certaines propriétés des racines, on

peut les utiliser pour découvrir le groupe de l'équation et, inversement, quand on connaît le groupe de l'équation, il en résulte certaines propriétés communes à toutes les équations de la classe à laquelle appartient ce groupe; nous allons maintenant montrer comment on parvient à la notion du groupe.

189. Nous nous donnerons l'équation réductible ou irréductible du degré n

$$f(x) = 0, \tag{1}$$

dont nous supposerons les racines toutes *inégales*

$$x_1, \quad x_2, \quad \ldots, \quad x_n.$$

Considérons une fonction des racines qui prenne des valeurs toutes distinctes quand on y permute ces racines; une pareille fonction a $n!$ valeurs, qui sont racines d'une équation de degré $n!$ sans racines égales. Nous pouvons, par exemple, prendre cette fonction égale à

$$y_1 = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n, \tag{2}$$

α_1, α_2, $\ldots$, α_n étant choisis de telle sorte que toutes les valeurs de y soient distinctes.

L'équation du degré $n!$ qui détermine les valeurs de y peut être réductible; décomposons-la en d'autres irréductibles et désignons l'une d'elles (la résolvante) par

$$\mathrm{F}(y) = 0. \tag{3}$$

Supposons-la de degré m.

Soient $y_1, y_2, \ldots, y_m$ ses racines. On a vu (74) que chacune de ces racines pouvait s'exprimer rationnellement en fonction de l'une d'entre elles; on a vu aussi (73) que toute racine de (1) pouvait s'exprimer rationnellement au moyen d'une quelconque des racines de (3).

On peut donc représenter les racines de (1) sous la forme

$$\Psi_1(y_1), \quad \Psi_2(y_1), \quad \ldots, \quad \Psi_n(y_1), \tag{4}$$

$\Psi_1, \Psi_2, \ldots, \Psi_n$ désignant des fonctions rationnelles. Désignons par A_1 la permutation (4) des racines représentées par cette série; si l'on change y_1 en y_k, A_1 se changera en une autre permutation A_k des racines $x_1, x_2, \ldots$, à savoir celle qu'on obtient au moyen de la substitution qui change y_1 en y_k (75). On obtient ainsi m permutations des lettres $x_1, x_2, \ldots, x_n$, à savoir

(5) $$A_1, \quad A_2, \quad \ldots, \quad A_m,$$

qui se déduisent de A_1 au moyen des substitutions

(6) $$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{m-1}.$$

Nous allons prouver que ces substitutions forment un groupe. On a, en effet,

$$y_k = \theta(y_1),$$

θ désignant une fonction rationnelle déterminée. La série A_k ou $S_{k-1}A_1$ pourra se mettre alors sous la forme

$$\Psi_1\theta y_1, \quad \Psi_2\theta y_1, \quad \ldots, \quad \Psi_n\theta y_1$$

[en écrivant θy_1 au lieu de $\theta(y_1)\ldots$] et, en opérant avec la substitution S_{q-1}, on obtiendra pour la série des $S_{q-1}S_{k-1}A_1$

$$\Psi_1\theta y_q, \quad \Psi_2\theta y_q, \quad \ldots, \quad \Psi_n\theta y_q;$$

car l'effet de la substitution S_{q-1} est de remplacer y_1 par y_q.

Si la suite de ces racines coïncide avec une des suites A, le produit $S_{q-1}S_{k-1}$ se trouvera dans la suite (6), et les substitutions de cette suite formeront un groupe.

Puisque $\theta(y_1) = y_k$ est une racine de l'équation irréductible (3), il faut que l'équation du degré m dont les racines sont $\theta(y_1), \theta(y_2), \ldots, \theta(y_m)$ coïncide avec (3), et l'on doit avoir, par exemple,

$$\theta(y_q) = y_r;$$

la série précédente coïncide alors avec la série A'.

Il est donc prouvé que les m substitutions (6) *forment un groupe. Ce groupe a été désigné par Galois sous le nom de* groupe de l'équation; *nous le désignerons par* G.

Propriétés du groupe d'une équation.

190. *Toute fonction rationnelle* U *des racines dont la valeur numérique n'est pas altérée par les substitutions du groupe* G *peut s'exprimer rationnellement au moyen des quantités connues.*

La fonction U peut s'exprimer rationnellement au moyen d'une des racines de (3), par exemple y_1, de telle sorte que l'on a

$$U = \varphi(y_1),$$

φ désignant une fonction rationnelle. Comme les substitutions de G n'altèrent pas la valeur de U et que leur effet est de permuter y_1 avec $y_2, y_3, \ldots, y_m$, on a aussi

$$U = \varphi(y_2) = \varphi(y_3) = \ldots = \varphi(y_m),$$

et, par suite,

$$U = \frac{1}{m}[\varphi(y_1) + \varphi(y_2) + \ldots + \varphi(y_m)].$$

U s'exprime ainsi comme fonction symétrique des racines de (3) et, par suite, peut s'obtenir au moyen des quantités connues.

191. *Une fonction rationnelle des racines qui peut s'exprimer rationnellement au moyen des quantités connues reste numériquement inaltérée par les substitutions du groupe* G.

Soit B la valeur donnée de la fonction ; en exprimant toutes les racines qui entrent dans B au moyen de y_1, on a

$$\varphi(y_1) = B,$$

φ désignant une fonction rationnelle ; y_1 est donc une racine de

$$\varphi(y) - B = 0,$$

qui doit, par suite, admettre les autres racines $y_2, y_3, \ldots, y_m$; on a donc

$$\varphi(y_2) = B, \qquad \varphi(y_3) = B, \qquad \ldots, \qquad \varphi(y_m) = B,$$

si bien que la fonction conserve la valeur B quand on effectue les substitutions de G.

Ce théorème est encore vrai et la démonstration conserve toute sa force quand B est irrationnel, pourvu que l'adjonction des irrationnelles contenues dans B n'empêche pas (3) d'être irréductible.

192. *Il n'y a que les substitutions du groupe* G *qui laissent invariables toutes les fonctions rationnelles des racines.*

Considérons, en effet, la fonction

$$(\alpha - y_1)(\alpha - y_2)\ldots(\alpha - y_m)$$

où α est indéterminé; on voit facilement que cette fonction, dont la valeur est rationnelle, ne reste inaltérée que par les substitutions permutant y_1, y_2, ..., y_m, c'est-à-dire par les substitutions du groupe G. Une équation ne peut donc avoir qu'un seul groupe; *on doit donc trouver le même groupe quelle que soit l'équation analogue à* (3) *dont on fait usage.* Ces équations par suite sont de même degré.

193. *Si deux fonctions rationnelles des racines,* φ *et* ψ *sont égales, elles ne cessent pas de l'être après avoir effectué une substitution du groupe* G.

Car leur différence est rationnelle; elle doit donc toujours conserver sa valeur nulle après que l'on a effectué les substitutions du groupe.

194. *Le groupe* G *est transitif ou intransitif, suivant que l'équation est irréductible ou non.*

Si le groupe est intransitif il échange quelques racines entre elles sans les échanger avec les autres; il ne change donc pas une fonction symétrique quelconque de ces racines; une semblable fonction peut donc s'exprimer rationnellement, et ces racines seront les racines d'une équation à coefficients rationnels; l'équation proposée est donc réductible.

D'un autre côté, si l'équation est réductible, on doit avoir, pour des racines déterminées,

$$(\alpha - x_1)(\alpha - x_2)\ldots(\alpha - x_p) = K,$$

où α est indéterminé et K rationnel; ce produit ne conserve sa valeur que si l'on permute ensemble $x_1, x_2, \ldots, x_p$, ou si l'on permute d'autres racines entre elles. G ne peut donc contenir que des substitutions produisant ces permutations, il est donc intransitif.

Si l'on ne garde, parmi les substitutions de G, que les cycles qui contiennent $x_1, x_2, \ldots, x_p$, on obtient un groupe G_1. Une fonction de ces racines, qui reste inaltérée par les permutations de G_1, mais qui est altérée par toutes les autres qui permutent $x_1, x_2, \ldots, x_p$, est rationnelle, car elle n'est pas altérée par les substitutions de G. G_1 est donc le groupe de l'équation qui a pour racines $x_1, x_2, \ldots, x_p$.

195. *La résultante provenant de l'élimination de y entre*

$$y^m + a_1 y^{m-1} + \ldots + a_m = 0$$

et

$$\varphi_0(y)x^n + \varphi_1(y)x^{n-1} + \ldots + \varphi_n(y),$$

où $a_1, a_2, \ldots$ sont rationnels et $\varphi_0, \varphi_1, \ldots$ sont des fonctions rationnelles, a son groupe imprimitif, et réciproquement toute équation dont le groupe est imprimitif provient d'une semblable élimination.

Soient $y_1, y_2, \ldots, y_m$ les racines de la première équation, soient $x_{\rho 1}, x_{\rho 2}, \ldots, x_{\rho n}$ les racines de la seconde quand on y remplace y par y_ρ; soit v_ρ une fonction symétrique arbitraire de ces n racines; la fonction

$$A = (\alpha - v_1)(\alpha - v_2)\ldots(\alpha - v_m),$$

où α est indéterminé, est alors une fonction symétrique de $y_1, y_2, \ldots, y_m$ et peut s'exprimer rationnellement. Le groupe cherché ne peut contenir que des substitutions laissant A invariable, c'est-à-dire laissant $v_1, v_2, \ldots, v_m$ invariables ou

les permutant entre eux. Ces substitutions échangent ainsi les n racines du système

$$x_{\rho 1}, \quad x_{\rho 2}, \quad \ldots, \quad x_{\rho n},$$

contre les n racines du même ou d'un autre système; le groupe est donc imprimitif.

D'un autre côté, soit G le groupe imprimitif d'une équation contenant les m systèmes de lettres

$$x_{\rho 1}, \quad x_{\rho 2}, \quad \ldots, \quad x_{\rho n},$$

pour $\rho = 1, 2, \ldots, m$. Posons

$$v_\rho = (\beta - x_{\rho 1})(\beta - x_{\rho 2})\ldots(\beta - x_{\rho n})$$

et

$$A = (\alpha - v_1)(\alpha - v_2)\ldots(\alpha - v_m),$$

où α et β sont indéterminés. A reste inaltéré par les substitutions qui remplacent des lettres d'un même système par des lettres d'un même système. A reste donc invariable par les substitutions du groupe et peut s'exprimer rationnellement. A l'aide de A on pourra trouver toutes les fonctions symétriques de $v_1, v_2, \ldots, v_m$ sous forme rationnelle; v, ayant les valeurs $v_1, v_2, \ldots, v_m$, sera ainsi déterminé par une équation de degré m à coefficients rationnels; quand v_ρ sera connu, x_ρ sera déterminé d'une manière analogue par une équation de degré n dont les coefficients seront des fonctions rationnelles de v_ρ.

Réduction du groupe au moyen de quantités adjointes.

196. L'ordre de G est le degré de l'équation irréductible en y; si l'on adjoint de nouvelles quantités de manière à rendre cette équation décomposable, on obtient un nouveau groupe d'ordre moindre; comme les substitutions du nouveau groupe sont déterminées par les racines de la nouvelle équation irréductible et que ces racines se trouvent parmi les quantités $y_1, y_2, \ldots, y_m$, le nouveau groupe est contenu dans l'ancien.

197. *Si l'on adjoint la valeur z_1 d'une certaine fonction rationnelle des racines, le groupe nouveau devient le groupe des substitutions de* G *qui n'altèrent pas* z_1.

z_1 ayant été adjoint doit être regardé comme rationnel; toute substitution du nouveau groupe doit laisser inaltérée la fonction z_1 des racines; le nouveau groupe est contenu dans l'ancien : donc il ne peut contenir que des substitutions de l'ancien groupe qui n'altèrent pas z_1.

Nous allons montrer que toutes les substitutions de G qui n'altèrent pas z_1 appartiennent au nouveau groupe; formons une fonction rationnelle quelconque des racines exprimable rationnellement au moyen de z_1 et des quantités connues, en appelant U_1 cette fonction et φ un symbole de fonction rationnelle

$$U_1 = \varphi(z_1),$$

d'où (193)

$$U_a = \varphi(z_a),$$

l'indice a indiquant que l'on a effectué une substitution quelconque a qui se trouve parmi celles de G qui n'altèrent pas z_1; on a donc

$$z_a = z_1 \qquad \text{et} \qquad U_a = U_1,$$

en sorte que la substitution a laisse invariables toutes les fonctions qui peuvent s'exprimer rationnellement en z_1 et des quantités connues. a appartient donc, en réalité, au nouveau groupe après l'adjonction de z_1.

198. *Si une fonction φ des racines et une autre fonction π restent inaltérées par les mêmes substitutions de* G, *φ peut s'exprimer rationnellement en fonction de π.*

En effet, si l'on adjoint π, on obtient pour l'équation un groupe réduit H. Ses substitutions laissent π et φ invariables, φ peut donc s'exprimer rationnellement au moyen de π et des quantités connues.

Adjonction des racines d'une équation auxiliaire.

199. Soit z_1 une racine d'une équation irréductible auxiliaire dont les racines sont $z_1, z_2, \ldots, z_k$; nous admettrons que l'adjonction de z_1 réduise le groupe G. Alors l'équation $F(y) = 0$ se décompose en d'autres irréductibles du même degré, chacune d'elles peut servir à déterminer le nouveau groupe; soit

$$(1) \qquad \varphi(y, z_1) = 0$$

l'une de ces équations; on peut supposer que le coefficient de la plus haute puissance de y soit l'unité, les autres étant des fonctions entières rationnelles de z_1 de degré $k-1$ au plus.

Si l'on divise $F(y)$ par $\varphi(y, z)$ et si l'on égale à zéro les coefficients du reste on obtient les conditions pour que $F(y)$ soit divisible par $\varphi(y, z)$; ces équations de condition sont satisfaites pour $z = z_1$ et comme l'équation en z est irréductible elles doivent être satisfaites pour $z = z_2, \ldots, z = z_k$, $F(y)$ est donc divisible par $\varphi(y, z_2), \ldots, \varphi(y, z_k)$.

Le produit

$$(2) \qquad \Psi(y) = \varphi(y, z_1)\,\varphi(y, z_2)\ldots\varphi(y, z_k)$$

est une fonction entière de y et des quantités connues (les valeurs de z ne sont pas ici regardées comme connues); chaque facteur étant facteur de $F(y)$, l'équation

$$(3) \qquad \Psi(y) = 0$$

ne saurait avoir d'autres racines que celles de $F(y) = 0$, et doit les admettre au même degré de multiplicité; donc on a identiquement

$$(4) \qquad \Psi(y) = [F(y)]^q.$$

Comme $\varphi(y, z_1) = 0$ est irréductible, les autres équations analogues le sont aussi, pourvu que pour chacune d'elles la valeur correspondante de z soit adjointe. Si, en effet, $\varphi(y, z)$

était divisible par $\varphi_1(y, z)$, pour $z = z$, le reste de la division de $\varphi(y, z)$ par $\varphi_1(y, z)$ devrait être nul pour $z = z_i$, il devrait encore être nul pour $z = z_1$ et $\varphi(y, z_1) = 0$ serait réductible, ce qui est en contradiction avec ce qui précède.

Lorsque deux des équations $\varphi = 0$ ont une racine commune, toutes leurs racines sont égales deux à deux; en effet, si

$$(5) \qquad \varphi(y, z_1) = 0 \quad \text{et} \quad \varphi(y, z_2) = 0$$

ont toutes deux la racine y_1, et si la première a, en outre, la racine y_2, y_2 pourra s'exprimer rationnellement en y_1, et l'on aura

$$(6) \qquad y_2 = \theta(y_1),$$

θ désignant une fonction rationnelle. L'équation

$$(7) \qquad \varphi[\theta(y), z_1] = 0$$

a alors une racine commune avec la première équation (5) et par suite doit les admettre toutes; la fonction

$$\varphi[\theta(y), z]$$

est alors divisible par $\varphi(y, z)$ pour $z = z_1$ et donc de même pour $z = z_2$, de sorte que l'équation

$$(8) \qquad \varphi[\theta(y), z_2] = 0$$

doit être satisfaite quand $\varphi(y, z_2) = 0$ l'est; parmi les racines de cette équation se trouve y_1, en sorte que l'on a identiquement

$$(9) \qquad \varphi[\theta(y_1), z_2] = 0 \quad \text{ou} \quad \varphi(y_2, z_2) = 0;$$

d'où il résulte que y_2 est racine de la seconde équation (5) : deux des équations $\varphi = 0$ ont donc ou les mêmes racines, ou toutes leurs racines différentes.

Soit y_1 une racine commune à q de ces équations, ces équations devront avoir les mêmes racines; q autres équations doivent avoir les mêmes racines, sans les avoir communes avec les équations du système précédent, et ainsi de suite.

En extrayant la racine $q^{\text{ième}}$ de (4), on a alors, identiquement,

$$(10) \qquad F(y) = \varphi(y, z_1)\,\varphi(y, z_2)\ldots\varphi(y, z_r),$$

où $\varphi(y, z_1), \ldots, \varphi(y, z_r)$ désignent des facteurs de chaque système; on a donc $k = qr$.

Les racines z se partagent ainsi en r systèmes de q racines, de telle sorte que l'on obtient deux groupes réduits différents, suivant que l'on adjoint deux racines appartenant à deux systèmes différents, tandis que l'on obtient le même groupe réduit pour deux racines d'un même système.

Dans le cas où le degré k de l'équation auxiliaire est un nombre premier p, on a $q = 1$. $F(y)$ est donc un produit de p facteurs et l'on obtient l'ordre du groupe réduit en divisant l'ordre de G par p.

Si l'on adjoint une fonction des racines d'une équation, on adjoint en définitive une racine de l'équation irréductible qui détermine cette fonction. Les valeurs de cette fonction forment alors des systèmes analogues à ceux que nous venons de considérer.

200. *Les différents groupes réduits sont semblables.*

Soient H_1 et H_2 deux de ces groupes correspondant à z_1 et z_2; soient y_1 et y_2 des racines respectives de

$$\varphi(y, z_1) = 0, \qquad \varphi(y, z_2) = 0.$$

Les racines de la première équation peuvent être mises sous la forme

$$y_1, \quad \theta_1(y_1), \quad \theta_2(y_1), \quad \ldots,$$

$\theta_1, \theta_2, \ldots$ désignant des fonctions rationnelles.

On montrera, comme plus haut, que les racines de la seconde sont

$$y_2, \quad \theta_1(y_2), \quad \theta_2(y_2), \quad \ldots.$$

Soit maintenant T la substitution qui remplace y_1 par y_2,

S_k, S'_k les substitutions qui remplacent y_1 par $\theta_k(y_1)$ et y_2 par $\theta_k(y_2)$; on a

$$TS_k = S'_k T;$$

car ces deux substitutions remplacent y_1 par $\theta_k(y_2)$; cette formule établit la similitude de S_k et S'_k; mais S_k est une substitution quelconque du groupe H_1, S'_k une substitution du groupe H_2; la substitution T transforme donc H_1 en H_2. Comme y_1 et y_2 sont des racines quelconques de (3), une substitution quelconque de G transformera un groupe H en lui-même ou en un autre groupe H.

201. *Si les racines de l'équation irréductible auxiliaire peuvent être exprimées rationnellement en fonction de l'une d'elles, et si l'adjonction d'une de ces racines réduit* G *à* H, H *sera permutable avec toutes les substitutions de* G.

Si toutes les racines de l'équation auxiliaire peuvent être exprimées rationnellement en fonction de l'une d'elles, en les exprimant effectivement ainsi, adjoindre une racine de l'équation auxiliaire, c'est les adjoindre toutes; les groupes H_1, H_2, ... que l'on a trouvés tout à l'heure doivent coïncider; mais, puisque tous ces groupes peuvent être transformés les uns dans les autres avec les substitutions de G, H transformé par ces substitutions reste identique à lui-même : H est donc permutable avec les substitutions de G.

202. *Si l'adjonction de toutes les racines d'une équation irréductible auxiliaire réduit le groupe* G *à* H, H *est permutable avec toutes les substitutions de* G.

L'adjonction des racines en question revient à l'adjonction d'une fonction φ rationnelle de ces racines, dont toutes les valeurs sont distinctes; ces valeurs peuvent être exprimées rationnellement en fonction de l'une d'elles, et les racines de l'équation auxiliaire peuvent être exprimées rationnellement en fonction de φ, de sorte que les racines de l'équation en φ peuvent être considérées comme adjointes; notre théorème résulte donc du précédent (201).

203. *Dans le cas où le groupe* G *d'ordre* $m = kq$ *contient un groupe* H *d'ordre* q, *permutable avec toutes les substitutions de* G, G *pourra se réduire à* H *en adjoignant les racines d'une équation abélienne de degré* k.

Soient

$$1, \quad S_1, \quad S_2, \quad \ldots, \quad S_{q-1}$$

les substitutions de H; les substitutions de G peuvent être distribuées en k séries : elles sont de la forme $T_\alpha S_\beta$, où α a la même valeur dans une même série.

Soient $y_1, y_2, \ldots, y_q$ les racines de $F(y) = 0$, qui se déduisent de y_1 pour les substitutions S, et soit

$$\theta_1 = (\alpha - y_1)(\alpha - y_2)\ldots(\alpha - y_q),$$

α désignant une indéterminée; θ_1 reste inaltéré par les substitutions S, mais les autres substitutions changent sa valeur; si donc on adjoint θ_1, le groupe de l'équation deviendra H.

Montrons maintenant que θ_1 peut être déterminé au moyen d'une équation abélienne. Soient $\theta_1, \theta_2, \ldots, \theta_k$ les valeurs que l'on obtient en effectuant sur θ_1 les substitutions $1, T_1, T_2, \ldots, T_{k-1}$, et posons

$$A = (\beta - \theta_1)(\beta - \theta_2)\ldots(\beta - \theta_k),$$

où β désigne une indéterminée.

Puisque H est permutable avec les substitutions de G, aucune des fonctions θ (181) ne sera altérée par les substitutions S. A ne peut donc être altéré par aucune substitution $T_\beta S_\alpha$; car S_α ne modifie aucune des valeurs θ, et T ne fait qu'échanger les valeurs des θ; on a, par exemple,

$$T_\beta \theta_3 = T_\beta T_2 \theta_1 = T_\gamma S_\delta \theta_1 = \theta_{\gamma+1};$$

car $T_\beta T_2$ fait partie du groupe G et doit avoir, à cause de cela, la forme $T_\gamma S_\delta$.

Puisque aucune substitution de G ne modifie A, A pourra s'exprimer rationnellement. $\theta_1, \theta_2, \ldots$ seront déterminés par une équation du degré k, et l'on voit facilement que cette équation est irréductible et abélienne, car les diverses va-

leurs de θ peuvent s'exprimer rationnellement les unes en fonction des autres, puisqu'elles restent invariables par les mêmes substitutions de G; leur groupe est d'ordre k et se compose des substitutions qui permutent θ_1, θ_2, ... de la même manière que les substitutions T.

Si k est un nombre premier, les racines de l'équation abélienne peuvent s'exprimer rationnellement au moyen d'une équation binome; on peut donc aussi réduire G à H en adjoignant un radical et les racines de l'unité.

204. A présent, nous pouvons faire connaître les conditions nécessaires et suffisantes pour qu'une équation puisse être résolue algébriquement. Si une équation peut être résolue algébriquement, son groupe doit pouvoir se réduire à la seule substitution 1, en adjoignant successivement les radicaux qui se trouvent dans les racines et des racines de l'unité, de manière à connaître toutes les racines de l'équation en y. Le groupe devra donc se réduire à 1 en adjoignant successivement des racines d'équations de la forme

$$z^p = A,$$

où p désigne un nombre premier et A une quantité connue ou déjà adjointe. Cette équation est abélienne si l'on regarde les racines de l'unité comme des quantités connues.

D'ailleurs, aux nos 199 et 203, on a montré que la condition nécessaire et suffisante pour que le groupe G de l'équation, d'ordre pq, puisse être réduit par une telle adjonction, consiste en ce que ce groupe G contienne un groupe H d'ordre q, permutable avec toutes les substitutions de G. Alors H doit contenir un nouveau groupe permutable avec toutes les substitutions de H, et ainsi de suite jusqu'à ce que l'on parvienne au groupe 1. Ainsi

La condition nécessaire et suffisante pour qu'une équation puisse être résolue algébriquement est que son groupe contienne un groupe et celui-ci un nouveau groupe, et ainsi de suite, jusqu'à ce que l'on parvienne au groupe 1; *et cette suite*

de groupes doit être telle que chacun d'eux soit permutable avec les substitutions du précédent, l'ordre de chacun d'eux s'obtenant en divisant l'ordre du précédent par un nombre premier.

205. Prenons, par exemple, l'équation générale du quatrième degré; son groupe est le groupe général du quatrième degré et du vingt-quatrième ordre; ce groupe contient le groupe alterné avec lequel ses substitutions sont permutables; en adjoignant une fonction altérée des racines, le groupe sera réduit au groupe alterné; c'est cette fonction que l'on trouve quand, cherchant à résoudre l'équation, on est conduit à extraire une première racine carrée.

Le groupe alterné contient un groupe du quatrième ordre où les substitutions sont permutables avec un groupe alterné; ce groupe est

$$1, \quad (x_1 x_2)(x_3 x_4), \quad (x_1 x_3)(x_2 x_4), \quad (x_1 x_4)(x_2 x_3).$$

Au moyen d'une extraction de racine cubique, on détermine une fonction qui reste inaltérée par ces substitutions, par exemple $x_1 x_2 + x_3 x_4$; si l'on adjoint cette fonction, le groupe alterné se trouve réduit au groupe du quatrième ordre considéré, qui, au moyen de deux extractions de racines carrées, se trouve réduit au groupe 1.

Le groupe général de degré n, qui est le groupe de l'équation générale de degré n, peut aussi, au moyen d'une extraction de racine carrée, être réduit au groupe alterné. Nous allons voir tout à l'heure que, pour $n > 4$, ce groupe est simple, et alors ce groupe ne peut plus être réduit par l'adjonction d'un radical; il en résulte que les équations générales de degré supérieur à 4 ne peuvent pas être résolues algébriquement.

Voici maintenant la démonstration de la proposition que nous avons admise : Supposons que le groupe G d'ordre $\frac{1}{2} n!$ puisse se réduire à un autre K d'ordre k où $kp = \frac{1}{2} n!$, p désignant un nombre premier. K ne saurait contenir toutes les substitutions circulaires du troisième ordre. On peut donc for-

mer un groupe d'ordre $3k$ (**161**) contenu dans G, ainsi $p=3$; si $n>4$, on peut montrer que $p=5$, K ne contenant pas toutes les substitutions circulaires du cinquième ordre; mais p ne peut être à la fois 3 et 5; la réduction est donc impossible pour $n>4$.

En réalité, cette démonstration ne diffère pas de celle que nous avons donnée plus haut pour établir que l'équation du cinquième degré n'était pas résoluble algébriquement.

CHAPITRE IV.

APPLICATIONS DE LA THÉORIE DE GALOIS.

Équations abéliennes.

206. Nous avons déjà étudié les équations abéliennes. Aussi montrerons-nous brièvement comment on peut leur appliquer la théorie de Galois.

Considérons une équation abélienne irréductible de degré n, on aura

$$(1) \qquad x_2 = \theta(x_1) \quad \text{ou} \quad x_2 - \theta(x_1) = 0;$$

le groupe de l'équation doit contenir une substitution qui remplace x_1 par x_2; soit

$$(x_1, x_2, x_3, \ldots, x_r)$$

un de ses cycles; si l'on fait subir à (1) cette substitution, on a

$$(2) \qquad \theta(x_1) = x_2, \quad \theta(x_2) = x_3, \quad \ldots, \quad \theta(x_r) = x_1.$$

On voit alors facilement qu'une substitution du groupe qui remplace une des lettres x_1, x_2, ..., x_r par une lettre qui ne fait pas partie de cet ensemble, doit les remplacer toutes par de nouvelles lettres, sans quoi l'équation aurait des racines égales; transformons une substitution entre les lettres x_1, x_2, ..., x_r par une substitution qui les échange avec d'autres, nous obtenons une substitution qui montre que r racines différentes des précédentes sont liées par des équations analogues aux fonctions (2); s'il y a plus de r racines, un autre

système de r racines sera encore lié par des équations analogues, etc., et les substitutions du groupe ne pourront échanger que des racines d'un même système avec des racines d'un même système. Le groupe est donc imprimitif et l'équation peut se décomposer en équations de degré r, au moyen d'une équation auxiliaire.

207. On n'a donc à considérer que des équations dont le groupe contient une substitution circulaire de toutes les racines et où $x_2 = \theta(x_1)$. Toutes les racines peuvent alors s'exprimer rationnellement en fonction de l'une d'elles, et une fonction des racines n'a que n valeurs. L'équation $F(y) = 0$, qui détermine le groupe, est donc au plus du degré n : elle est donc exactement de degré n, car le groupe est transitif et, par suite, son ordre est divisible par n. Ce groupe se compose d'une substitution circulaire et de ses puissances.

Soit α une racine primitive de $\alpha^n = 1$, on voit facilement que

$$A = (\alpha x_1 + \alpha^2 x_2 + \ldots + x_n)^n$$

est rationnel, car cette fonction n'est pas altérée par les substitutions du groupe. Si l'on adjoint α et $\sqrt[n]{A}$, le groupe sera réduit à l'unité; les autres substitutions changent, en effet, $\alpha x_1 + \alpha^2 x_2 + \ldots + x_n$; les racines seront donc exprimables rationnellement en fonction de $\sqrt[n]{A}$ et des racines de l'unité.

Si le degré d'une équation abélienne est un nombre premier n, son groupe doit contenir une substitution circulaire d'ordre n; l'équation sera alors résoluble algébriquement. Si n n'est pas premier, et si le groupe contient encore une substitution circulaire d'ordre n, on voit que l'on peut abaisser son groupe en adjoignant des radicaux à indices premiers; par exemple, si $n = 15$ et si S est la substitution circulaire,

$$1, \quad S^3, \quad S^6, \quad S^9, \quad S^{12}$$

sera un groupe permutable avec les substitutions du groupe primitif, et sera le groupe réduit en adjoignant les racines d'une équation de la forme

$$z^3 = A.$$

Équations de Galois.

208. Galois a étudié les équations irréductibles de degré premier p et dont les racines sont exprimables rationnellement en fonction de deux d'entre elles, et il a fait voir qu'elles sont résolubles algébriquement.

Toute fonction rationnelle des racines d'une pareille équation pouvant s'exprimer rationnellement en fonction de deux racines, l'ordre de son groupe est au plus $p(p-1)$, et comme ce groupe est transitif, son ordre est divisible par p.

Nous avons vu plus haut (186) que les substitutions d'un groupe de cette espèce, les racines étant $x_0, x_1, x_2, \ldots, x_{p-1}$ sont de la forme

$$\begin{pmatrix} az+b \\ z \end{pmatrix}$$

ou de la forme

$$T^\alpha S^\beta,$$

où

$$S = \begin{pmatrix} z+1 \\ z \end{pmatrix}; \qquad T = \begin{pmatrix} az \\ z \end{pmatrix}.$$

L'ordre du groupe est kp, k est égal à $p-1$ ou à un diviseur de $p-1$, et a est une racine primitive de $a^k \equiv 1 \pmod p$.

Maintenant, posons

$$X_1 = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{p-1} x_{p-1})^p,$$

où α est racine de $\dfrac{x^p-1}{x-1} = 0$, désignons par $X_2, X_3, \ldots, X_{k-1}$ les résultats obtenus en effectuant sur X_1 les substitutions $T, T^2, \ldots, T^{k-1}$, et posons encore

$$A = (X_1 + \beta X_2 + \beta^2 X_3 + \ldots + \beta^{k-1} X_k)^k,$$

β désignant une racine quelconque de $x^k - 1 = 0$. A doit être rationnel, car il n'est pas altéré par les substitutions du groupe, car la substitution S n'altère pas $X_1, X_2, \ldots, X_k$ et la substitution T effectue des permutations circulaires entre les X.

Si l'on remplace alors β par ses différentes valeurs, on obtient k équations qui se ramènent au premier degré et d'où l'on peut tirer $X_1, X_2, \ldots$ en fonction de $\sqrt[k]{X}$ et des racines de l'unité.

Les quantités $X_1, X_2, \ldots$ étant connues, on en déduit x_0, $x_1, \ldots$ comme on l'a vu à propos des équations abéliennes. En réalité l'équation donnée se réduit à une équation abélienne par l'adjonction d'une de ces quantités, car alors le groupe se réduit aux puissances de S. Donc :

Une équation irréductible dont le degré est un nombre premier, et dont les racines sont des fonctions rationnelles de deux d'entre elles peut se résoudre algébriquement.

Dans le cas où le groupe d'une équation irréductible de degré p ne contient que des substitutions linéaires, chaque racine peut s'exprimer en fonction rationnelle de deux d'entre elles; car si l'on adjoint deux racines, le groupe se trouve réduit à l'unité, puisque, mise à part la substitution 1, les substitutions linéaires déplacent au moins $p-1$ racines et ne peuvent en laisser deux invariables.

209. *Si une équation irréductible dont le degré est un nombre premier p est résoluble algébriquement, son groupe ne contient que des substitutions linéaires.*

Si l'on adjoint tous les radicaux, pour réduire le groupe de l'équation, il se trouvera un radical d'indice p, car c'est le seul qui pourra faire disparaître le facteur p de l'ordre du groupe. Dès que l'on aura adjoint ce radical, et pas avant, l'équation sera réductible, et comme le nouveau groupe est intransitif, son ordre ne peut être divisible par p, et réciproquement l'équation ne peut être irréductible si l'on n'a pas évincé le facteur p de l'ordre du groupe.

L'équation donnée devient donc réductible après l'adjonction du radical d'indice p, et son groupe est devenu intransitif ou réduit à l'unité. Soit

$$H = (1, U_1, U_2, \ldots)$$

ce groupe. Avant l'adjonction du radical, le groupe contenait toutes les substitutions de la forme

$$S^{\alpha}U_{\beta},$$

S désignant une substitution circulaire d'ordre p (161).

Les lettres se distribuent en systèmes, de telle sorte que les substitutions U n'échangent que des lettres d'un même système; H est permutable avec les puissances de S; celles-ci ne peuvent donc échanger que des lettres d'un même système avec des lettres d'un même système; comme ce n'est pas le cas pour les puissances de S, H ne peut contenir que la substitution 1. La dernière adjonction doit être d'un radical d'indice p et auparavant le groupe était composé d'une substitution circulaire et de ses puissances.

Comme le groupe se trouve réduit à l'unité par la dernière adjonction, toutes les racines deviennent rationnelles, de sorte que l'équation auparavant irréductible se décompose actuellement en équations du premier degré.

210. Les adjonctions successives auraient pu réduire le groupe sans rendre $f(x) = 0$ réductible; dans le cas où des adjonctions réduisent le groupe G à H qui ne contient que des substitutions linéaires, on peut montrer que G ne contient non plus que des substitutions linéaires, et le théorème précédent en résultera, car, le dernier groupe ne contenant que des substitutions linéaires, cela aura lieu pour les autres.

Il reste donc à prouver que G ne peut contenir que des substitutions linéaires, si le groupe H, obtenu par l'adjonction des racines d'une équation binome, ne contient lui-même que des substitutions linéaires. H doit contenir la substitution circulaire S d'ordre p et ses puissances; soit T une substitution de G qui n'entre pas dans H, H est permutable avec T, et T doit par suite transformer S en une de ses puissances, car dans le groupe linéaire H il n'entre pas d'autre substitution semblable à S que les puissances de S. T est donc lui-même une substitution linéaire, car seules les substitutions linéaires transforment S en une puissance de S.

Il est donc prouvé que la condition donnée par Galois pour la résolubilité d'une équation irréductible de degré premier, sous forme algébrique, est nécessaire et suffisante.

Équations dont le groupe a pour ordre une puissance d'un nombre premier.

211. Soit p^n l'ordre du groupe d'une équation irréductible $f(x) = 0$, p désignant un nombre premier. Comme l'ordre du groupe est divisible par le degré de l'équation, ce degré doit être une puissance de p, p^m par exemple.

Si l'on adjoint une racine x_1 de l'équation, l'équation devient réductible; chacune des équations irréductibles dans lesquelles elle se décompose a un groupe qui ne contient que des substitutions dont l'ordre est une puissance de p (194), de sorte que ces groupes ont pour ordre une puissance de p et il en est de même des degrés des équations correspondantes.

Puisque l'équation se trouve réduite par l'adjonction de x_1 à d'autres dont les degrés sont des puissances de p et que parmi ces équations il en est une du premier degré, il faut qu'il y en ait au moins p du premier degré; au moins p racines seront rationnellement exprimables en fonction de x_1. Plus haut (206) on a fait voir que le groupe de semblables équations était imprimitif et qu'elles pouvaient être réduites au moyen d'une équation auxiliaire. Le groupe de l'équation réduite se compose de substitutions dont les cycles se trouvent dans les substitutions de G, et leur ordre comme le degré de l'équation sont des puissances de p.

En divisant le degré de l'équation proposée par celui de l'équation réduite, on a le degré de l'équation auxiliaire (195), qui par suite est aussi une puissance de p. L'ordre du groupe de l'équation auxiliaire est aussi une puissance de p, car ce groupe se réduit à l'unité en adjoignant toutes les racines de l'équation donnée. Adjoignons ces racines une à une; à chaque réduction on doit parvenir à une équation irréductible dont l'ordre du groupe et le degré doivent être une puissance de p. On voit ainsi que l'ordre du groupe de l'équation auxiliaire

doit être une puissance de p (199). On arrive au même résultat en montrant que ce groupe est isomorphe avec G.

Les deux nouvelles équations peuvent être réduites de la même façon jusqu'à ce que l'on tombe sur des équations abéliennes de degré p. Comme le produit des degrés de ces équations est égal au degré de la proposée, les racines de celle-ci peuvent être exprimées au moyen de m équations abéliennes d'ordre p.

212. D'un autre côté, l'ordre du groupe d'une équation, qui peut être résolue à l'aide d'équations abéliennes de degré p, peut être abaissé au moyen de divisions successives par le nombre p, jusqu'à ce qu'il se réduise à l'unité; l'ordre de ce groupe est donc une puissance de p. Donc

La condition nécessaire et suffisante pour qu'une équation puisse être résolue au moyen d'équations abéliennes de degré p est que l'ordre de son groupe soit une puissance de p. Son degré est alors nécessairement une puissance de p également.

Ce théorème est une généralisation de celui qui fait connaître les conditions pour qu'une équation soit résoluble au moyen de racines carrées, et que nous avons démontré plus haut.

La démonstration qui précède montre qu'il n'y a pas d'autres groupes transitifs d'ordre p^n $(n > 1)$ que des groupes imprimitifs. Cela résulte nettement de ce qu'il existe une équation qui possède un groupe donné. En effet, chaque groupe correspond à une équation; à savoir l'équation générale de même degré que le groupe quand on a adjoint une fonction des racines invariable par les substitutions du groupe et variable par tout autre substitution.

213. Supposons qu'un groupe G contienne un groupe H d'ordre p^α, p désignant un nombre premier. Toutes les substitutions de G permutables avec H forment un groupe K d'ordre μp^α.

Supposons

$$H = (1, S_1, S_2, \ldots);$$

les substitutions de K peuvent être rangées en séries, de la forme

$$T_\gamma, \quad T_\gamma S_1, \quad \ldots;$$

dans le cas où H est celui des sous-groupes contenus dans G pour lequel α est le plus grand possible, il ne peut se trouver, parmi les substitutions $T_\gamma S_\beta$, une substitution dont l'ordre soit une puissance de p; s'il s'en trouvait en effet une, on pourrait à l'aide de cette substitution construire un groupe contenu dans Q, et d'ordre p^β où $\beta > \alpha$ (161); comme l'ordre de chaque substitution S est une puissance de p, elle ne peut être semblable à une substitution TS.

Les substitutions de G peuvent être rangées en séries comme il suit (chaque série a μp^α termes) :

$$\begin{array}{l} 1, \quad S_1, \quad S_2, \quad \ldots, \quad T, \quad TS_1, \quad \ldots. \\ U, \quad US_1, \quad US_2, \quad \ldots, \quad UT, \quad \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

U n'est pas permutable avec H, mais il pourrait l'être avec un groupe contenu dans H, à savoir $1, S_\alpha, S_\beta, \ldots$; les substitutions S peuvent être écrites en séries comme il suit

$$\begin{array}{l} 1, \quad S_\alpha, \quad S_\beta, \quad \ldots, \\ M_1, \quad M_1 S_\alpha, \quad M_1 S_\beta, \quad \ldots, \\ M_2, \quad M_2 S_\alpha, \quad M_2 S_\beta, \quad \ldots, \end{array}$$

le nombre des substitutions M étant une puissance de p.

Si l'on multiplie à gauche les termes de la série

$$U, \quad US_1, \quad US_2, \quad \ldots, \quad UT, \quad \ldots$$

par l'une des substitutions $S_\alpha, S_\beta, \ldots$, on retrouve la même série à l'ordre des termes près. Au contraire, si l'on multiplie les termes de la même série par une des substitutions M, on obtient une nouvelle série, composée de termes différant à la fois entre eux et de ceux de la série primitive. On déduit ainsi de la série primitive autant de séries qu'il y a de substitutions M; le nombre de ces séries est une puissance de p.

Si G contient un plus grand nombre de substitutions, avec l'une d'elles formons de la même manière une série de substitutions dont le nombre soit une puissance de p, et continuons ainsi jusqu'à ce que nous ayons épuisé toutes les substitutions de G. Comme toutes les substitutions ainsi obtenues sont différentes, l'ordre de G est

$$\mu p^{\alpha}(1 + p^{\alpha-\alpha_1} + p^{\alpha-\alpha_2} \ldots),$$

où p^{α_1}, p^{α_2}, ... sont les ordres des groupes contenus dans H et qui sont permutables avec les substitutions U. Plusieurs des nombres α_1, α_2, ... peuvent être égaux; ils peuvent même être nuls, mais ils sont au plus égaux à $\alpha - 1$. La quantité entre parenthèses a en tout cas la forme $1 + np$.

214. Nous allons étudier de plus près le groupe K et montrer que μ ne peut être divisible par p. Puisque H est permutable avec toutes les substitutions de K, on peut, si l'on considère une équation dont le groupe est K, réduire K à H, au moyen d'une équation auxiliaire du degré μ dont toutes les racines peuvent être exprimées rationnellement à l'aide de l'une d'entre elles, et dont le groupe est d'ordre μ (203). Ce groupe doit contenir une substitution d'ordre p, si μ est divisible par p.

Cette substitution, par rapport aux quantités désignées (203) par θ_1, θ_2, ..., peut être remplacée par une des substitutions T (203); la puissance p de cette substitution doit laisser θ_1, θ_2, ... inaltérées. Comme cela n'a lieu que pour les substitutions S, T^p est l'une d'elles, ce qui exigerait que l'ordre de T fût une puissance de p, ce qui est contraire à notre hypothèse. μ n'est donc pas divisible par p.

On voit ainsi qu'un groupe d'ordre kp^{α}, où k n'est pas divisible par p, doit contenir un sous-groupe imprimitif d'ordre p^{α} ou un groupe linéaire d'ordre p si $\alpha = 1$. Le groupe d'ordre p^{α} est contenu dans un autre d'ordre μp^{α} avec les substitutions duquel il est permutable, et l'on a

$$k = \mu(np + 1).$$

215. Si $k < p$, on a $k = \mu$; soit alors $\mu = \mu_1 p_1^\beta$, où p_1 désigne un nouveau nombre premier qui ne divise pas μ_1. Si $\mu_1 < p_1$, l'équation auxiliaire de degré μ pourra être réduite à une équation résoluble par radicaux, au moyen d'une équation de degré μ_1; si l'on peut ainsi continuer jusqu'à ce que l'on obtienne une équation auxiliaire dont le degré et l'ordre soient des puissances d'un nombre premier, l'équation proposée est résoluble algébriquement (Sylow, *Math. Annalen*, V).

Équation de Hesse.

216. Hesse a étudié une équation du neuvième degré, dans laquelle deux racines quelconques a, b sont liées à une troisième par les relations

$$c = \varphi(a, b), \qquad b = \varphi(a, c), \qquad a = \varphi(b, c),$$

φ désignant une fonction symétrique et rationnelle.

On rencontre cette équation quand on cherche les 9 points d'inflexion d'une courbe du troisième degré. Au sujet de ces points on a le théorème suivant : toute droite passant par deux points d'inflexion passe par un troisième point d'inflexion. La condition pour que trois de ces points soient en ligne droite prend la forme $c = \varphi(a, b)$, où a, b, c sont trois racines de l'équation du neuvième degré qui détermine les points d'inflexion. L'équation $c = \varphi(a, b)$ n'est satisfaite que si les trois points a, b, c sont en ligne droite.

217. Le groupe de l'équation ne peut contenir que des substitutions qui remplacent les trois points a, b, c par trois autres en ligne droite (193).

On peut prendre deux points sur neuf de 72 manières; de cette manière chaque droite est obtenue 6 fois, et il existe 12 lignes droites distinctes passant par trois inflexions. On arrive au même résultat en observant que par chaque point passent 4 des lignes en question; leur nombre est donc $4 \times 9 : 3 = 12$.

De 3 points en ligne droite partent donc 9 lignes droites, abstraction faite de celle-ci; les 6 autres points se trouvent donc sur les deux droites restantes.

Maintenant représentons chaque point d'inflexion par deux indices; le premier de ces indices sera 0, 1 ou 2 suivant que le point sera sur la première, la deuxième ou la troisième de ces lignes; sur les 9 lignes restantes choisissons-en 3 de la même façon et donnons au point le second indice 0, 1 ou 2 suivant qu'il sera sur la première, la deuxième ou la troisième. De cette manière les points seront représentés par les éléments du tableau

$$\begin{array}{ccc} (00) & (01) & (02), \\ (10) & (11) & (12), \\ (20) & (21) & (22); \end{array}$$

les points représentés par les éléments d'une même ligne ou d'une même colonne sont alors en ligne droite.

On ne peut ranger ces points de manière à voir les 6 autres lignes parce que 3 points d'inflexion au plus sont réels. Les deux lignes droites que l'on ne voit pas et qui passent par le point (00) sont nécessairement

$$\begin{array}{ccc} (00) & (11) & (22), \\ (00) & (12) & (21); \end{array}$$

les autres lignes sont déterminées d'une façon analogue, et l'on voit que si 3 points sont en ligne droite la somme de leurs premiers et de leurs seconds indices est divisible par 3.

218. Désignons ces indices par x et y, et considérons les substitutions qui remplacent x et y par $ax + by + c$ et $a_1x + b_1y + c_1$, les nombres étant pris suivant le module 3; alors, après la substitution, 3 points en ligne droite seront remplacés par 3 autres points encore en ligne droite, car si

$$x_1 + x_2 + x_3 \equiv y_1 + y_2 + y_3 \equiv 0,$$

on a encore

$$ax_1 + by_1 + c + ax_2 + by_2 + c + ax_3 + by_3 + c \equiv 0.$$

La notation

$$(x, y;\quad ax + by + c,\quad a_1 x + b_1 y + c_1)$$

représentera une substitution des 9 points, si l'on exclut les valeurs de a, b, a_1, b_1 pour lesquelles $ab_1 - ba_1 \equiv 0$. Ces substitutions forment un groupe, car le produit de deux d'entre elles donne une substitution de même espèce. c et c_1 peuvent être pris égaux à 0, 1 ou 2; si c et c_1 ont été choisis, a et b ne doivent pas être à la fois nuls; si a et b ont été choisis, a_1 et b_1 peuvent être choisis de 6 manières différentes; l'ordre du groupe est donc 9.8.6.

Le groupe en question remplace 3 points en ligne droite par 3 autres points en ligne droite; nous allons voir qu'il contient toutes les substitutions qui jouissent de cette propriété.

Soit T une semblable substitution qui remplace (00) par $(\alpha\beta)$, (01) par $(\alpha_1\beta_1)$, elle devra remplacer (02) par (α_2, β_2), de telle sorte que

$$\alpha + \alpha_1 + \alpha_2 \equiv \beta + \beta_1 + \beta_2 \equiv 0;$$

la substitution

$$S = (x, y;\quad ax + by + \alpha,\quad a_1 x + b_1 y + \beta_1)$$

du groupe produit cet effet quand

$$b + \alpha \equiv \alpha_1, \qquad b_1 + \beta \equiv \beta_1;$$

si T remplace (10) par $(\alpha_3\beta_3)$, la substitution S produira cet effet si

$$a + \alpha \equiv \alpha_3, \qquad a_1 + \beta \equiv \beta_3.$$

On voit facilement que la substitution T est maintenant bien déterminée, et cela par cette seule condition que 3 points en ligne droite sont remplacés par 3 autres en ligne droite; et comme la substitution S déterminée jouit de cette propriété, S et T sont égales.

G contient ainsi les substitutions qui n'altèrent pas la valeur nulle de $\varphi(a, b) - c$. Alors G est le groupe de l'équation ou le contient.

G contient le groupe G_1 formé des substitutions

$$(x, y;\quad ax + c,\quad ay + c_1),$$

où a est égal à 1 ou 2, et où c et c_1 peuvent recevoir leurs trois valeurs. Ce groupe du dix-huitième ordre est permutable à toutes les substitutions de G. Si l'on cherche 3 droites contenant les 9 inflexions, on voit que G_1 ne contient que les substitutions de G qui échangent ces lignes; comme il existe 12 lignes triples et qu'une ligne triple détermine les deux autres, il existe 4 lignes triples qui doivent se déterminer au moyen d'une équation du quatrième degré dont les racines réduisent le groupe G à G_1.

On peut encore réduire le groupe G à G_1 en résolvant une équation abélienne du degré $9.8.6 \div 18 = 24$. Cette équation n'est autre chose que la résolvante de l'équation du quatrième degré et se trouve résolue dès que celle-ci l'est. Au lieu de réduire le groupe G à G_1 pour la fonction des racines, on aurait pu le réduire par l'adjonction successive des radicaux qui servent à résoudre l'équation du quatrième degré.

On divise ainsi l'ordre de G par 24.

G_1 contient le groupe G_2 du troisième ordre

$$(x, y;\quad x, y + c_1)$$

qui est permutable avec les substitutions de G_1; le groupe Q_1 peut être réduit à G_2, en adjoignant les racines d'une équation du troisième degré qui fait connaître les 3 droites d'un triple, ou en adjoignant les radicaux qui servent à résoudre cette équation.

Le groupe est alors réduit aux puissances d'une substitution régulière du troisième ordre; il est donc intransitif, et l'équation se trouve réduite à 3 équations du troisième degré; ces équations sont abéliennes, le groupe se trouvant réduit à 1 en adjoignant une racine arbitraire.

Groupe de monodromie d'une équation.

220. Soit

$$f(x, k) = 0$$

une équation contenant un paramètre indéterminé k; pour plus de simplicité, nous supposerons les coefficients numériques. Si l'on suppose k connu, l'équation possède un groupe déterminé G.

Une fonction rationnelle φ de k et des racines qui reste inaltérée par les substitutions de G peut être exprimée rationnellement au moyen de k et des nombres connus; elle doit donc être *monodrome* par rapport à k, c'est-à-dire qu'elle doit avoir une valeur déterminée pour une valeur donnée de k, et reprendre cette même valeur quand k, après avoir varié d'une manière quelconque, repasse par sa valeur primitive. La fonction reprend après la variation de k sa valeur numérique primitive, mais sa forme algébrique peut avoir changé, la variation de k pouvant avoir amené une permutation entre les racines.

Si l'on fait varier k en lui faisant prendre toutes les valeurs réelles ou imaginaires, on produira des substitutions entre les racines; ces substitutions forment un groupe, car si k en suivant un chemin fermé produit une substitution S et en suivant un autre chemin fermé il produit la substitution T, en suivant successivement ces deux chemins il produira la substitution TS. Ce groupe porte le nom de *groupe de monodromie* par rapport à k. Nous le désignerons par H.

221. *Les substitutions du groupe de monodromie n'altèrent pas une fonction monodrome de k.* En effet, si k suit un chemin déterminé, il en résulte une substitution déterminée correspondante, et, comme la fonction est monodrome, cette substitution ne le change pas, puisque la fonction reprend la même valeur quand k revient au même point, quel que soit le chemin suivi.

Réciproquement, une fonction est monodrome quand elle n'est pas altérée par les substitutions de H. Car ces substitutions correspondent à tous les chemins que peut suivre k.

222. *Le groupe* H *est contenu dans* G. Toutes les substitutions de H laissent, en effet, une valeur rationnelle d'une fonction rationnelle des racines et de k inaltérée, car cette fonction est monodrome.

Mais il faut remarquer que H ne contiendra nécessairement pas toutes les substitutions de G; en effet, de ce qu'une fonction est monodrome, il n'en résulte pas qu'elle puisse s'exprimer rationnellement par des quantités connues ; elle peut, par exemple, contenir des radicaux et G ne se réduit à H qu'après l'adjonction de ces radicaux.

223. *Le groupe* H *est permutable aux substitutions de* G.

Soit ψ une fonction des racines invariable par les substitutions de H, mais variable par les autres substitutions. Elle sera monodrome en k et par suite exprimable rationnellement au moyen de k et de coefficients irrationnels; appelons $a, b, c, \ldots$ ces coefficients; la fonction ψ satisfait à une équation irréductible ; on obtiendra des relations entre $a, b, c, \ldots$ en écrivant que ψ satisfait, quel que soit k, à cette équation. On peut donc former une équation telle que $a, b, c, \ldots$ s'expriment rationnellement au moyen d'une de ses racines (74), et, si l'on adjoint ses racines, G se réduira à un groupe qui ne pourra contenir d'autres substitutions que celles de H. Ce groupe sera donc H, car l'adjonction d'irrationnelles numériques ne saurait réduire ce groupe. H est donc permutable avec les substitutions de G (202).

224. Considérons, par exemple, l'équation qui fait connaître $\cos\frac{z}{n}$ au moyen de $k = \cos z$. Appelons $x_1, x_2, \ldots, x_n$ ses racines, où $x_p = \cos\frac{z+2p\pi}{n}$; adjoignons $\cos z$ et $\sin z$; si z varie d'une manière continue, $\cos z$ et $\sin z$ reprennent les

mêmes valeurs quand z croît de $2p\pi$, p désignant l'un des nombres $0, 1, 2, \ldots, n-1$; la racine x_r se changeant alors en x_{r+p}, le groupe de monodromie de l'équation par rapport à $\sin z$ et $\cos z$ est le groupe linéaire de degré n

$$\begin{pmatrix} r+p \\ r \end{pmatrix},$$

et, comme ce groupe est permutable avec les substitutions du groupe algébrique, celui-ci a la forme

$$\begin{pmatrix} ar+p \\ r \end{pmatrix};$$

il se réduit au groupe de monodromie en adjoignant $\cos\frac{2\pi}{n}$ et $\sin\frac{2\pi}{n}$, car on voit facilement que dans ce cas

$$\psi(x_{p+1}, x_p) = 0,$$

où ψ est rationnel et cette équation ne subsiste que pour les substitutions du groupe de monodromie.

CINQUIÈME PARTIE.

SUR LES FORMES.

COVARIANTS DES FORMES BINAIRES.

Formes et substitutions linéaires.

1. Nous désignerons par a_x^n la forme binaire générale d'ordre n

$$(1) \quad a_x^n = a_0 x_1^n + \frac{n}{1} a_1 x_1^{n-1} x_0 + \frac{n(n-1)}{1.2} a_2 x_1^{n-2} x_0^2 + \ldots + a_n x_0^n,$$

où $a_0, a_1, \ldots, a_n$ seront ce que nous appellerons les *coefficients;* si l'on fait $a_x^n = 0$, et si l'on regarde $x_1 : x_0$ comme inconnue, on obtient l'équation générale du degré n.

2. La forme est transformée par une substitution linéaire, quand on pose

$$(2) \qquad x_1 = \alpha_{11}\xi_1 + \alpha_{12}\xi_0, \qquad x_0 = \alpha_{21}\xi_1 + \alpha_{22}\xi_2,$$

et l'on suppose le déterminant

$$(3) \qquad D = \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix}$$

différent de zéro; si l'on a plusieurs formes analogues a_x^n, $b_x^{n_1}$, ..., il sera sous-entendu qu'elles sont transformées par la même substitution.

Quand on effectue la substitution, la forme se change en une autre de même ordre, mais avec de nouveaux coefficients a'_0, a'_1, ... qui dépendent des anciens et des coefficients de la substitution (2); on peut effectuer deux substitutions successivement : cela revient à effectuer une seule

substitution, mais cette troisième substitution n'est pas la même quand on change l'ordre dans lequel on effectue les deux premières; toutefois, le déterminant de la troisième est, en tout cas, le produit des déterminants des deux premières.

3. La substitution la plus générale résulte des quatre suivantes (*voir* 41) :

1° $x_1 = k\xi_1, \qquad x_0 = k\xi_0,$

2° $x_1 = \xi_1, \qquad x_0 = l\xi_0,$

3° $x_1 = \xi_1 + \alpha_1\xi_0, \qquad x_0 = \xi_0,$

4° $x_1 = \xi_1, \qquad x_0 = \alpha_2\xi_1 + \xi_0$

dont les déterminants sont k^2, l, 1 et 1. La substitution obtenue en les effectuant successivement aura pour déterminant $k^2 l$; c'est la plus générale, parce qu'elle contient les quatre paramètres k, l, α_1, α_2, et l'on voit facilement qu'on peut les déterminer sans ambiguïté quand on se donne les coefficients de (2). Excepté pourtant lorsque $\alpha_{11} = 0$ ou $\alpha_{22} = 0$; alors, en effet, ils sont infinis; comme, dans ce cas, α_{12} et α_{21} ne peuvent être nuls, nous admettrons encore une cinquième substitution simple qui échange seulement les variables; elle a pour déterminant -1 et change a_q en a_{n-q}.

Symboles.

4. Nous regarderons les lettres a, b, ..., A, B, ..., dans ce qui va suivre, comme des symboles dont les puissances seront remplacées par des indices; ainsi nous aurons

$$(a)^n = a_n, \qquad (a)^0 = a_0, \qquad (\mathrm{A})^3 = \mathrm{A}_3, \qquad \ldots,$$

mais n sera toujours égal à ou inférieur à l'ordre de la forme, car a_n n'a plus de sens dans le cas contraire. Nous pouvons alors écrire

$$(4) \qquad a_x^n = (x_1 + a x_0)^n,$$

si, après avoir appliqué la formule du binome, nous écrivons,

au lieu du premier terme,

$$x_1^n (a x_0)^0 = x_1^n (a)^0 (x_0)^0 = a_0 x_1^n.$$

Nous considérerons ensuite une différentiation symbolique pour laquelle nous ferons usage de la caractéristique Δ_1; elle consistera à appliquer les règles ordinaires de la différentiation aux puissances symboliques. Ainsi, on posera

$$\Delta_1 a_p = \Delta_1 (a)^p = p(a)^{p-1} = p a_{p-1}.$$

On voit donc que l'on n'a qu'à différentier en regardant les indices comme des exposants. Nous donnerons encore quelques exemples :

$$\Delta_1 a_p^m = m a_p^{m-1} \Delta_1 a_p = p m a_p^{m-1} a_{p-1}, \qquad \Delta_1 a_0 = 0,$$
$$\Delta_1 (a_1 a_2 - a_1^2) = 0, \qquad \Delta_1 a_1 a_3^2 = a_0 a_3^2 + 6 a_1 a_2 a_3.$$

Coefficients et fonctions transformés.

5. Lorsque l'on transforme la forme (1), on obtient une forme de même ordre avec de nouveaux coefficients a'_0, a'_1, ..., et il en est de même pour toute autre forme. Soit u une fonction entière et rationnelle des variables et des coefficients d'une ou de plusieurs fonctions, homogène en x_1 et x_0. Si, dans u, nous remplaçons les coefficients par ceux des formes transformées et x_1, x_0 par ξ_1, ξ_0 respectivement, nous obtenons une nouvelle expression u'. Maintenant, dans u', remplaçons les nouveaux coefficients et les variables ξ_1 et ξ_0 par leurs valeurs en fonction des anciens coefficients et des anciennes variables; si alors u' ne diffère de u que par un facteur dépendant seulement des coefficients de la substitution, on dira que u est un *covariant* de la forme, ou un *covariant simultané* des formes s'il intervient plusieurs formes dans l'expression de u. Les considérations qui vont suivre ont pour objet la recherche des covariants et leur mode de dépendance. Pour obtenir des covariants, nous chercherons les conditions pour que u reste invariable quand on

effectue les cinq substitutions particulières dont il a été question plus haut.

6. La première substitution donne

$$a'_q = k^n a_q, \qquad \xi_1 = x_1 : k, \qquad \xi_0 = x_0 : k.$$

On voit que tout covariant de a_x^n doit être homogène par rapport aux coefficients de cette forme; si son degré par rapport aux variables (que l'on appelle son *ordre*) est p, si son degré par rapport aux coefficients (que l'on appelle son *degré*) est g, la substitution considérée multiplie le covariant par k^{ng-p}. Si l'on considère un covariant de plusieurs formes des degrés $n, n_1, n_2, \ldots$, et si les degrés d'un de ses termes par rapport aux coefficients de ces formes sont respectivement g, g_1, $g_2, \ldots$, Σng sera le degré de tous ses termes et le covariant sera multiplié par $k^{\Sigma ng-p}$ après la transformation.

7. La seconde transformation donne

$$a'_q = l^q a_q, \qquad b'_q = l^q b_q, \qquad \xi_1 = x_1, \qquad \xi_0 = x_0 : l.$$

Si l'on désigne par ν le degré de A dans un terme $A x_1^\alpha x_0^\beta$, en y regardant les indices comme des exposants (c'est ce que l'on appelle le *poids* de A), ce terme sera multiplié par $l^{\nu-\beta}$; $\nu - \beta$ doit alors avoir la même valeur pour tous les termes d'un covariant. Si l'on ordonne le covariant comme les formes, le poids de chaque coefficient devra être supérieur d'une unité au poids du coefficient précédent.

8. La cinquième substitution change a_{n-q} en a_q, x_1 en x_0 et *vice versa;* ce changement ne doit pas altérer un covariant, ou doit simplement le multiplier par -1. Soit

$$(5) \qquad A_0 x_1^p + \frac{p}{1} A_1 x_1^{p-1} x_0 + \ldots + A_p x_0^p$$

le covariant, la substitution change A_0 en $\pm A_p$. Si ν est le poids de A_0, A_p sera de poids $\nu + p$.

Mais $A_0 A_p$ doit être de poids Σng, car, si dans $A_0 A_p$ il entre

un facteur a_p ou b_q, il doit aussi y entrer un facteur a_{n-p}, b_{n_1-q}, ... On a donc

$$(6) \qquad p = \Sigma ng - 2\nu,$$

ce qui montre que l'ordre d'un covariant est déterminé quand on connaît le poids et le degré de son premier coefficient.

Si l'on effectue successivement la première et la deuxième substitution, le covariant est multiplié par $k^{\Sigma ng - p} l^{\nu} = (k^2 l)^{\nu}$. Or $k^2 l$ est le déterminant de la substitution résultant des deux premières, la troisième et la quatrième substitution ont pour déterminant 1 et ne changent pas le covariant, comme nous le verrons plus loin; il en résulte que :

Une substitution quelconque de déterminant D *multiplie un covariant par* D^{ν}, ν *désignant le poids du premier coefficient du covariant.*

9. Nous avons vu que tous les coefficients d'un même covariant u ont le même poids ou, comme nous le disons, sont homogènes en indice et sont de même degré, c'est-à-dire homogènes dans le sens propre du mot. On aura donc, en vertu de cette dernière propriété,

$$a_0 \frac{\partial u}{\partial a_0} + a_1 \frac{\partial u}{\partial a_1} + \ldots + a_n \frac{\partial u}{\partial a_n} = gu.$$

L'homogénéité en indice fournit une équation analogue. Si nous faisons, en effet,

$$a_q = x_q^q, \qquad b_q = y_q^q,$$

nous aurons

$$\nu u = \sum x_q \frac{\partial u}{\partial x_q} + \ldots = \sum q x_q^q \frac{\partial u}{q x_q^{q-1}\, \partial x_q} + \ldots = \sum q x_q^q \frac{\partial u}{\partial x_q^q} + \ldots$$
$$= \sum q a_q \frac{\partial u}{\partial a_q} + \ldots$$

ou

$$(7) \qquad a_1 \frac{\partial u}{\partial a_1} + 2a_2 \frac{\partial u}{\partial a_2} + \ldots + n a_n \frac{\partial u}{\partial a_n} + b_1 \frac{\partial u}{\partial b_1} + \ldots = \nu u.$$

10. La troisième substitution est

$$x_1 = \xi_1 + \alpha_1 \xi_0, \qquad x_0 = \xi_0,$$

elle change $a_x^n = (x_1 + a x_0)^n$ en

$$[\xi_1 + (a + \alpha_1)\xi_0]^n.$$

Les coefficients de la forme transformée dépendent donc de ceux de la forme primitive au moyen d'une équation symbolique qui exprime que le symbole reçoit l'accroissement α_1. On a alors

$$(8)\qquad a'_p = (a + \alpha_1)^p = a_p + \frac{p}{1} a_{p-1}\alpha_1 + \frac{p(p-1)}{1.2} a_{p-2}\alpha_1^2 + \ldots + \alpha_1^p,$$

ce que l'on peut encore écrire

$$(9)\qquad a'_p = a_p + \Delta_1 a_p \frac{\alpha_1}{1} + \Delta_1^2 a_p \frac{\alpha_1^2}{1.2} + \ldots,$$

où Δ_1^2 représente $\Delta_1 \Delta_1$.

Nous avons là une analogie frappante avec la formule de Taylor et, si nous observons que cette dernière formule peut se démontrer en s'appuyant sur ce fait qu'elle est valable pour a^p et l'accroissement α_1 donné à a, et qu'on peut la généraliser en considérant plusieurs variables recevant des accroissements divers, on pourra l'étendre à des symboles; si nous supposons que tous ces symboles reçoivent le même accroissement α_1, la formule de Taylor donnera

$$u' = u + \left(\frac{\partial u}{\partial a} + \frac{\partial u}{\partial b} + \ldots\right)\alpha_1 + \ldots,$$

et, en faisant usage de la notation différentielle symbolique,

$$(10)\qquad u' = u + \Delta_1 u \frac{\alpha_1}{1} + \Delta_1^2 u \frac{\alpha_1^2}{1.2} + \ldots,$$

u désignant une fonction entière des coefficients d'un nombre quelconque de formes et u' la fonction transformée.

Si les variables entrent aussi dans u, on a

$$\xi_1 = x_1 - \alpha_1 x_0, \qquad \xi_0 = x_0,$$

et l'on trouve

$$(11)\qquad u' = u + \left(\Delta_1 u - x_0 \frac{\partial u}{\partial x_1}\right) \alpha_1 + \left(\Delta_1 u - x_0 \frac{\partial u}{\partial x_1}\right)^2 \frac{\alpha^2}{1.2} + \ldots,$$

formule dans laquelle les exposants des parenthèses doivent être considérés comme plus haut.

La formule (11) montre que les covariants doivent satisfaire à la relation

$$(12)\qquad \Delta_1 u - x_0 \frac{\partial u}{\partial x_1} = 0,$$

d'où il résulte

$$u' = u.$$

Si x_0 et x_1 n'entrent pas dans u, on a seulement

$$(13)\qquad \Delta_1 u = 0$$

ou

$$(14)\qquad a_0 \frac{\partial u}{\partial a_1} + 2 a_1 \frac{\partial u}{\partial a_2} + \ldots + n a_{n-1} \frac{\partial u}{\partial a_n} + b_0 \frac{\partial u}{\partial b_1} + \ldots$$

Au surplus, (12) peut être considérée comme un cas particulier de (13), si l'on y considère $-x_0$ et x_1 comme les coefficients d'une forme adjointe du premier degré.

11. La différentiation symbolique abaisse d'une unité le poids de chaque terme, sans changer les lettres; pour un covariant u, les termes de (12) qui contiennent les mêmes lettres au même degré doivent se détruire entre eux. Nous pouvons en conclure qu'un covariant est homogène par rapport aux coefficients de toutes les formes ou se décompose en plusieurs autres. Un covariant pourrait aussi se rapporter à des formes contenant des variables différentes, $x_0, x_1; y_0, y_1 \ldots;$ il devrait alors être homogène par rapport à chaque paire de variables, et dans (12) il s'introduirait de nouveaux termes de la forme

$$-y_0 \frac{\partial u}{\partial y_1}.$$

12. La quatrième substitution transforme a_x^n en

$$[\xi_1(1+a\alpha_2)+a\xi_0]^n,$$

alors

$$a'_p=(1+a\alpha_2)^{n-p}a^p=a_p+\frac{n-p}{1}a_{p+1}\alpha_2+\ldots$$
$$=a_p+\Delta_2 a_p\frac{\alpha_2}{1}+\Delta_2^2 a_p\frac{\alpha_2^2}{1.2}+\ldots,$$

Δ_2 désignant une opération identique avec Δ_1, à cela près que a_q doit être remplacé par a_{n-q}, b_q par b_{n_1-q}, ... On a donc

$$\Delta_2 a_0=na_1,\qquad \Delta_2 a_q=(n-q)a_{q+1},$$
$$\Delta_2 a_{n-1}=a_n,\qquad \Delta_2 a_n=0.$$

La condition pour que u soit un covariant est alors

$$\Delta_2 u-x_1\frac{\partial u}{\partial x_0}=0, \tag{15}$$

et l'on a, en général,

$$u'=u+\left(\Delta_2 u-x_1\frac{\partial u}{\partial x_0}\right)\frac{\alpha_2}{1}+\left(\Delta_2 u-x_1\frac{\partial u}{\partial x_0}\right)^2\frac{\alpha_2^2}{1.2}+\ldots, \tag{16}$$

formule qui doit être généralisée comme (11), si l'on a affaire à plusieurs paires de variables. Si les variables n'entrent pas dans u, (15) donne

$$\Delta_2 u=0 \tag{17}$$

ou

$$0=na_1\frac{\partial u}{\partial a_0}+(n-1)a_2\frac{\partial u}{\partial a_1}+\ldots+a_n\frac{\partial u}{\partial a_{n-1}}+n_1b_1\frac{\partial u}{\partial b_0}+\ldots. \tag{18}$$

13. Nous allons maintenant montrer comment les coefficients d'un covariant dépendent de l'un d'entre eux. Soit le covariant

$$K=A_0x_1^\mu+\frac{\mu}{1}A_1x_1^{\mu-1}x_0+\frac{\mu(\mu-1)}{1.2}A_2x_1^{\mu-2}x_0^2+\ldots+A_\mu x_0^\mu+\ldots. \tag{19}$$

Supposons que g soit le degré et ν le poids de A_0, de sorte que

$$\mu = ng - 2\nu.$$

Nous avons vu que A_q est de degré g et de poids $\nu + q$.

Si nous appliquons à K la formule (12), nous trouvons

$$\Delta_1 A_0 x_1^\mu + \frac{\mu}{1}\Delta_1 A_1 x_1^{\mu-1} x_0 + \frac{\mu(\mu-1)}{1.2}\Delta_1 A_2 x_1^{\mu-2} x_0^2 + \ldots + \Delta_1 A_\mu x_0^\mu$$
$$- \frac{\mu}{1} A_0 x_1^{\mu-1} x_0 - \frac{\mu(\mu-1)}{1} A_1 x_1^{\mu-2} x_0^2 - \ldots - \mu A_{\mu-1} x_0^\mu$$

et, comme cette quantité doit être identiquement nulle,

$$\Delta_1 A_0 = 0, \qquad \Delta_1 A_1 = A_0, \qquad \Delta_1 A_2 = 2A_1, \qquad \ldots, \qquad \Delta_1 A_q = q A_{q-1}.$$

On voit que *l'opération* Δ_1 *a le même effet sur les coefficients d'un covariant et sur ceux de la forme.*

Appliquons à K la formule (15), nous trouvons

$$\Delta_2 A_0 x_1^\mu + \frac{\mu}{1}\Delta_2 A_1 x_1^{\mu-1} x_0 + \frac{\mu(\mu-1)}{1.2}\Delta_2 A_2 x_1^{\mu-2} x_0^2 + \ldots + \Delta_2 A_\mu x_0^\mu$$
$$- \frac{\mu}{1} A_1 x_1^\mu - \frac{\mu(\mu-1)}{1} A_2 x_1^{\mu-1} x_0$$
$$- \frac{\mu(\mu-1)(\mu-2)}{1.2} A_3 x_1^{\mu-2} x_0^2 - \ldots - \frac{\mu}{1} A_\mu x_1 x_0^{\mu-1},$$

d'où l'on conclut

$$\Delta_2 A_p = 0, \qquad \Delta_2 A_{p-1} = A_p, \qquad \ldots,$$
$$\Delta_2 A_q = (\mu - q) A_{q+1}, \qquad \ldots, \qquad \Delta^2 A_0 = \mu A_1.$$

Ces formules montrent que *l'opération* Δ_2 *s'applique d'après les mêmes règles aux coefficients d'un covariant et aux coefficients d'une forme de même ordre que le covariant.*

De ces théorèmes, il résulte qu'*un covariant est entièrement déterminé quand on connaît un quelconque de ses coefficients*, car au moyen des deux opérations on peut déterminer tous les autres. En particulier nous remarquerons que A_0 satisfait à l'équation $\Delta_1 A_0 = 0$ et A_μ à l'équation $\Delta_2 A_\mu = 0$. Les fonctions qui satisfont à ces deux équations

seront ce que nous appellerons des *semi-invariants;* ils seront de première espèce ou de seconde espèce, suivant qu'ils satisferont à la première ou à la seconde ([1]).

Un covariant d'ordre nul satisfait aux deux conditions et on l'appelle un *invariant;* pour un semblable covariant, on a $\Sigma ng = 2\nu$. Les deux espèces de semi-invariants se déduisent les uns des autres en changeant a_q en a_{n-q}, b_q en b_{n_1-q}, ... Il en résulte qu'un invariant, par un semblable changement, doit rester inaltéré ou changer seulement de signe selon que son poids est pair ou impair; car le changement se produit par la cinquième transformation.

Les covariants deviennent des invariants lorsque l'on regarde les variables comme coefficients de formes linéaires dont le premier terme est négatif.

Semi-invariants.

14. On voit facilement que

$$(a_1 - aa_0)^\mu$$

est un semi-invariant de première espèce, car

$$\Delta_1 (a_1 - aa_0)^\mu = \mu (a_1 - aa_0)^{\mu-1} (a_0 - a_0) = 0;$$

il se trouve représenté par $a_x^\mu = (x_1 + ax_0)^\mu$, si l'on remplace x_1 par a_1 et x_0 par $-a_0$. Il est nul identiquement pour $\mu = 1$; pour les autres valeurs de μ, on a, en divisant par a_0, qui est lui-même un semi-invariant,

$$(20)\qquad c_0 = a_0, \qquad c_2 = a_0 a_2 - a_1^2, \qquad c_3 = a_0^2 a_3 - 3 a_0 a_1 a_2 + 2 a_1^3;$$

n est la plus grande valeur que puisse prendre μ.

A l'aide de ces $n - 1$ semi-invariants, on peut exprimer en fonction entière tous les semi-invariants de a_x^n, après les avoir multipliés par une puissance convenable de a_0.

([1]) Parfois, quand nous parlerons de semi-invariants, sans en désigner l'espèce, il faudra sous-entendre qu'il s'agit de semi-invariants de première espèce.

Dans c_μ, le premier terme est $a_0^{\mu-1} a_\mu$, et a_μ n'entre que dans ce terme. On peut alors éliminer d'un semi-invariant donné U, au moyen des équations (20), les quantités a_n, a_{n-1}, a_{n-2}, ..., a_2 et l'on n'introduit ainsi que des dénominateurs puissances de a_0; on obtient ainsi

$$U = A + B a_1 + C a_1^2 + \ldots,$$

A, B, C, ... désignant des fonctions entières des c divisées par des puissances de c_0. A, B, C, ... sont ainsi eux-mêmes des semi-invariants et l'on a

$$\Delta_1 U = B a_0 + 2 C a_0 a_1 + \ldots,$$

et cette quantité n'est identiquement nulle que quand $B = C \ldots = 0$, car les c et a peuvent être considérés comme indépendants.

On voit, de même, qu'une fonction U, telle que $\Delta_1^2 U = 0$, peut être ramenée à la forme $A + B a_1$, etc.

D'une manière toute semblable on verrait que des semi-invariants simultanés, abstraction faite de multiplicateurs puissances de a_0, b_0, ..., peuvent être exprimés en fonction entière et rationnelle des c et de leurs analogues ainsi que de semi-invariants de la forme $a_0 b_1 - b_0 a_1$. Enfin, on aurait des théorèmes analogues pour des semi-invariants de seconde espèce en changeant a_q en a_{n-q}, etc.

15. Il est facile de trouver l'expression d'un semi-invariant donné de a_x^n en fonction des c. Si l'on pose, en effet, $a_1 = 0$, c_μ se réduit à $a_0^{\mu-1} a_\mu$; il suffit alors de multiplier le semi-invariant par une puissance de a_0 telle que son degré devienne égal à son poids (tous les c, excepté c_0, jouissent de cette propriété), et alors de poser $a_1 = 0$; on a ainsi l'expression demandée.

Par exemple, soit

$$d_4 = a_0 a_4 - 4 a_1 a_3 + 3 a_2^2, \qquad \Delta_1 d_4 = 0,$$

en multipliant par a_0^2 et en posant $a_1 = 0$, on a

$$a_0^3 a_4 + 3 (a_0 a_2)^2,$$

d'où l'on tire

$$d_4 = \frac{c_4 + 3c_2^2}{c_0^2}.$$

C'est ce que l'on peut voir d'une autre manière.

Le semi-invariant doit rester inaltéré par la troisième substitution, et par suite quand on remplace a_q par

$$a_q + q a_{q-1} \alpha_1 + \ldots,$$

comme α_1 doit disparaître du résultat, on peut le remplacer par une quantité arbitraire; nous le remplacerons par $-\frac{a_1}{a_0}$. Si nous multiplions par a_0^ν, où ν désigne le poids, a_q se change en $a_0 c_q$, et si l'on divise par a_0^g, où g désigne le degré, on retrouve le résultat auquel nous sommes parvenus tout à l'heure.

On aurait pu remplacer α_1 par $\frac{x_1}{x_0}$; et en multipliant par une puissance de x_0, a_q se serait changé en a_x^q; donc :

Un semi-invariant quelconque, multiplié par une puissance convenable de x_0, peut s'exprimer sous forme entière au moyen de a_x^n, a_x^{n-1}, ...

Par exemple, on a identiquement

$$x_0^4(a_0 a_4 - 4a_1 a_3 + 3a_2^2) = a_0 a_x^4 - 4a_x^1 a_x^3 + 3(a_x^2)^2.$$

Ce théorème s'étend sans difficulté aux semi-invariants simultanés. On a, par exemple,

$$x_0(a_0 b_1 - b_0 a_1) = a_0 b_x^1 - b_0 a_x^1.$$

16. On obtient encore un groupe de semi-invariants en posant

$$d_\mu = (a - b)^\mu,$$

car on a

$$\Delta_1 d_\mu = \mu(a-b)^{\mu-1}(1-1) = 0.$$

Si l'on pose $b = a$, on obtient des semi-invariants relatifs

à la forme a_x^n, qui, pour μ impair, s'évanouissent identiquement; ainsi

$$(21)\qquad \begin{cases} d_2 = a_0 a_2 - a_1^2, \\ d_4 = a_0 a_4 - 4 a_1 a_3 + 3 a_2^2, \\ d_6 = a_0 a_6 - 6 a_1 a_5 + 15 a_2 a_4 - 10 a_3^2, \\ \dots\dots\dots\dots\dots\dots\dots\dots \end{cases}$$

Ces quantités peuvent servir, au lieu de c_2, c_4, ..., à exprimer un semi-invariant; et, par ce nouveau procédé, on introduira en dénominateur une puissance moins élevée de a_0.

17. Il est facile de trouver la signification des semi-invariants c; en effet, si en appliquant la troisième substitution on pose α_1 égal à $-\frac{a_1}{a_0}$, le second terme de la forme transformée s'évanouit et a'_p se réduit à $\left(a - \frac{a_1}{a_0}\right)^p$ qui, abstraction faite du facteur a_0^{p-1}, se réduit à c_p; donc :

Si l'on transforme la forme de telle sorte que son second terme s'évanouisse, on trouve

$$a_0 \xi_1^n + \binom{n}{2} \frac{c_2}{a_0} \xi_1^{n-2} \xi_0^2 + \binom{n}{3} \frac{c_3}{a_0^2} \xi_1^{n-3} \xi_0^3 + \ldots + \frac{c_n}{a_0^{n-1}} \xi_0^n.$$

Si l'on égale cette forme à zéro, on obtient une équation dont les fonctions symétriques des racines pourront s'exprimer au moyen de $\frac{c_2}{a_0^2}$, $\frac{c_3}{a_0^3}$, ..., $\frac{c_n}{a_0^n}$; ses racines dépendent des différences des racines de l'équation non transformée; on a, en effet,

$$x_1 = \xi_1 - \frac{a_1}{a_0} \xi_0, \qquad x_0 = \xi_0 \qquad \text{et} \qquad \frac{x_1}{x_0} = \frac{\xi_1}{\xi_0} - \frac{a_1}{a_0}$$

où

$$-\frac{n a_1}{a_0} = \Sigma \frac{x_1}{x_0}.$$

Ainsi

$$\frac{\xi_1}{\xi_0} = \frac{1}{n} \Sigma \delta,$$

δ désignant la différence entre $\frac{x_1}{x_0}$ et une autre racine.

En ce qui concerne les semi-invariants de seconde espèce, il n'y a qu'à remplacer les racines par leurs inverses. D'ailleurs, il est facile de voir que la troisième substitution ne change pas la différence de deux racines et que la quatrième ne change pas la différence de leurs inverses.

18. Si l'on remplace α_1 par $-\frac{A_1}{A_0}$, A_0 et A_1 désignant les deux premiers coefficients d'un covariant, on trouve

$$a'_p = \left(a - \frac{A_1}{A_0}\right)^p;$$

c'est un semi-invariant qui, multiplié par A_0^p, est ramené à la forme entière. On obtient ainsi $n-1$ nouveaux semi-invariants par lesquels, à l'aide de A_0, un semi-invariant quelconque, multiplié par une puissance convenable de A_0, peut s'exprimer sous forme entière et rationnelle. A_0, comme nous le verrons, est un semi-invariant arbitraire qui n'est pas un invariant; si l'on exprime de même A_0, on obtient une relation entre les semi-invariants dont on a fait usage.

En effet, comme celui qui correspond à c_1 ne s'évanouit pas, on a, dans ce cas, n semi-invariants, tandis qu'il n'existe que $n-1$ semi-invariants c.

19. Il existe entre les opérations Δ_1 et Δ_2 une dépendance que l'on met en évidence comme il suit: on a

$$\Delta_1 u = \Sigma \mu a_{\mu-1} \frac{\partial u}{\partial a_\mu}, \qquad \Delta_2 u = \Sigma (n-\mu) a_{\mu+1} \frac{\partial u}{\partial a_\mu};$$

si l'on forme $\Delta_1 \Delta_2 u$ et $\Delta_2 \Delta_1 u$, on voit immédiatement que les termes qui renferment des dérivées du second ordre sont les mêmes; les autres sont

$$\Sigma(\mu+1)(n-\mu) a_\mu \frac{\partial u}{\partial a_\mu} \qquad \text{et} \qquad \Sigma \mu (n-\mu+1) a_\mu \frac{\partial u}{\partial a_\mu}.$$

On a donc, quel que soit le semi-invariant u,

$$(22) \qquad \Delta_1 \Delta_2 u - \Delta_2 \Delta_1 u = (ng - 2\nu) u.$$

Si u contient les coefficients de plusieurs formes, on doit remplacer ng par Σng.

Covariants.

20. Nous avons vu que les coefficients d'un covariant devaient satisfaire aux deux séries de relations

$$\Delta_1 A_q = q A_{q-1}, \qquad \Delta_2 A_q = (\mu - q) A_{q+1}.$$

En outre, on a

$$\Sigma ng - 2\nu = \mu,$$

μ désignant l'ordre du covariant, g le degré et ν le poids de A_0.

Nous pouvons montrer que la dernière condition peut remplacer une des séries de conditions trouvées plus haut, pourvu que nous ayons encore égard aux relations

$$\Delta_1 A_0 = 0 \quad \text{ou} \quad \Delta_2 A_\mu = 0.$$

On a, en effet,

$$\Delta_2 A_0 = \mu A_1 \quad \text{ou} \quad \Delta_1 \Delta_2 A_0 = \mu \Delta_1 A_1;$$

mais

$$\Delta_1 \Delta_2 A_0 = \Delta_2 \Delta_1 A_0 + (\Sigma ng - 2\nu) A_0 = \mu A_0;$$

donc

$$\Delta_1 A_1 = A_0.$$

De plus, on a

$$\Delta_2 A_1 = (\mu - 1) A_2, \qquad \Delta_1 \Delta_2 A_1 = (\mu - 1) \Delta_1 A_2,$$

mais

$$\begin{aligned}\Delta_1 \Delta_2 A_1 &= \Delta_2 \Delta_1 A_1 + (\Sigma ng - 2\nu - 2) A_1 \\ &= \Delta_2 A_0 + (\mu - 2) A_1 = 2(\mu - 1) A_1,\end{aligned}$$

donc

$$\Delta_1 A_2 = 2 A_1,$$

et ainsi de suite.

Tout semi-invariant détermine donc un et un seul covariant.

Le semi-invariant a_0 détermine la forme donnée (la forme fondamentale).

Il en résulte que les covariants dépendent les uns des autres de la même manière que les semi-invariants qui les déterminent. Si l'on a, par exemple,

$$A_0 = B_0 C_0 + D_0,$$

et si l'on remplace B_0, C_0 et D_0 par les covariants qu'ils déterminent, on obtient un covariant dont le premier terme a pour coefficient A_0, ce covariant n'est autre que celui qui est déterminé par A_0, car il n'y en a qu'un qui soit ainsi déterminé.

Les théorèmes démontrés plus haut, sur les semi-invariants, en donnent d'autres analogues pour les covariants; ainsi l'on a, par exemple, le théorème suivant :

Un covariant appartenant à la forme a_x^n, multiplié par une puissance convenable de la forme fondamentale, peut s'exprimer en fonction entière et rationnelle au moyen des covariants déterminés par les c.

On démontre des théorèmes analogues au sujet des semi-invariants de seconde espèce.

21. Nous avons montré plus haut que les semi-invariants sont simplement multipliés par une puissance de x_0 quand on y remplace a_μ par a_x^μ; il existe un théorème analogue pour les covariants. En effet, un covariant n'est pas altéré par la troisième substitution; on a donc identiquement

$$K = A'_0 (x_1 - \alpha_1 x_0)^\mu + \frac{\mu}{1} A'_1 (x_1 - \alpha_1 x_0)^{\mu-1} + \ldots + A'_\mu x_0^\mu,$$

ou, en remplaçant α_1 par $x_1 : x_0$,

$$K = A'_\mu x_0^\mu,$$

où A'_μ représente la valeur transformée de A_μ. Le changement dont nous avons parlé remplace a_μ par $a_x^\mu : x_0^\mu$, en sorte

que A'_μ acquiert le dénominateur $x_0^{\nu+\mu}$ où ν désigne le poids de A_0; ainsi :

Un covariant multiplié par x_0^ν est représenté par son dernier coefficient dans lequel on remplace a_p, b_q, ... par a_x^p, b_x^q, ...

On arrive au même résultat en donnant dans A_p au symbole l'accroissement $-\frac{x_1}{x_0}$ et en développant par la formule symbolique de Taylor.

Exemple. — A l'aide de c_2 et pour $n=4$, on forme un covariant d'ordre

$$2.4-4=4,$$

on a

$$A_0=a_0 a_2-a_1^2, \quad 2A_1=a_0 a_3-a_1 a_2, \quad 6A_2=a_0 a_4+2a_1 a_3-3a_2^2,$$
$$2A_3=a_1 a_4-a_2 a_3, \quad A_4=a_2 a_4-a_3^2,$$

et le covariant peut s'écrire

$$[a_x^4 a_x^2-(a_x^3)^2]:x_0^2;$$

pour $n=2$, c_2 est un invariant qui peut s'écrire

$$[a_0 a_x^2-(a_x^1)^2]:x_0^2;$$

pour $n=3$, c_2 donne le covariant

$$(a_0 a_2-a_1^2)x_1^2+(a_0 a_3-a_1 a_2)x_1 x_0+(a_1 a_3-a_2^2)x_0^2$$
$$=[a_x^1 a_x^3-(a_x^2)^2]:x_0^2.$$

Formation de nouveaux semi-invariants.

22. Étant donné un semi-invariant, on peut en déduire de nouveaux, en remplaçant les coefficients a_0, a_1, a_2, ... par une série de fonctions A_0, A_1, A_2, ... pour lesquelles

$$\Delta_1 A_0=0, \quad \Delta_1 A_1=A_0, \quad \Delta_1 A_2=2A_1, \quad \ldots.$$

En vertu de ces équations la nouvelle expression s'évanouira quand on la différentiera symboliquement, tout comme l'ancienne. Alors on peut remplacer a_q par a_q+kb_q, k désignant une constante arbitraire et b_q le coefficient d'une forme

adjointe. Un semi-invariant H se transformera en

$$\mathrm{H} + \left(\frac{\partial \mathrm{H}}{\partial a_0} b_0 + \frac{\partial \mathrm{H}}{\partial a_1} b_1 + \ldots \right) k + \ldots,$$

et comme k est arbitraire, les coefficients de toutes les puissances de k devront être des semi-invariants. Ainsi, un semi-invariant H en donne un autre

$$(23) \qquad \frac{\partial \mathrm{H}}{\partial a_0} b_0 + \frac{\partial \mathrm{H}}{\partial a_1} b_1 + \ldots + \frac{\partial \mathrm{H}}{\partial a_n} b_n;$$

la différentiation symbolique donne

$$(24) \qquad \Delta_1 \frac{\partial \mathrm{H}}{\partial a_0} = -\frac{\partial \mathrm{H}}{\partial a_1}, \quad \Delta_1 \frac{\partial \mathrm{H}}{\partial a_1} = -2 \frac{\partial \mathrm{H}}{\partial a_2}, \quad \ldots, \quad \Delta_1 \frac{\partial \mathrm{H}}{\partial a_n} = 0.$$

La dernière équation montre que d'un semi-invariant on peut en déduire un autre en différentiant par rapport au dernier coefficient a_n.

Les équations (24) montrent encore que chaque dérivée partielle détermine la suivante; H est donc bien déterminée quand on connaît $\frac{\partial \mathrm{H}}{\partial a_0}$ et en vertu de (7) quand on connaît $\frac{\partial \mathrm{H}}{\partial a_1}$ (et l'on en dirait autant des semi-invariants simultanés).

On voit encore que si a_μ entre dans H, $a_{\mu-1}$, $a_{\mu-2}$, ..., a_0 doivent y entrer également. Dans un invariant, à cause de la symétrie, il doit entrer tous les coefficients.

Si, dans un covariant, on regarde $-x_1$ et x_0 comme les coefficients d'une forme adjointe $-x_0 z_1 + x_1 z_0$, de telle sorte que $\Delta_1 x_1 = -x_0$; $\Delta_2 x_0 = -x_1$, les conditions de covariance deviennent des conditions d'invariance. On peut donc considérer les x comme des coefficients et les y comme de nouveaux coefficients; du covariant K on déduit alors le nouveau covariant

$$(25) \qquad y_1 \frac{\partial \mathrm{K}}{\partial x_1} + y_0 \frac{\partial \mathrm{K}}{\partial x_0},$$

divisé par le degré de K en x; on lui donne le nom de *pre-*

mière polaire de K. Si $K = A_x^p = (x_1 + Ax_0)^p$ on a, pour expression de cette polaire,

$$y_1(x_1 + Ax_0)^{p-1} + Ay_0(x_1 + Ax_0)^{p-1} = A_x^{p-1} A_y^1.$$

La première polaire de cette expression est la *seconde polaire* de K; elle a pour expression $A_x^{p-2} A_y^2$ et ainsi de suite; d'ailleurs les polaires de K se réduisent à K si l'on fait $y_1 = x_1$, $y_0 = x_0$.

Soit, maintenant, K_1 un covariant, avec deux paires de variables x et y et de degré r en y. Si l'on remplace y par x, on obtient un covariant K; soit R la $r^{\text{ième}}$ polaire de K, $K_1 - R$ doit alors s'annuler pour $y = x$ (c'est-à-dire pour $y_0 = x_0$, $y_1 = x_1$) et par suite il doit être divisible par $x_1 y_0 - y_1 x_0$ que l'on appelle le *covariant identique* et que l'on désigne par (xy). On a alors

$$K_1 = R + (xy)K_2,$$

où K_2 désigne un covariant dont le degré en x et en y est inférieur d'une unité au degré de K_1; si l'on traite K_2 comme K_1, et ainsi de suite, on a le théorème suivant :

Un covariant qui contient deux paires de variables x et y peut se mettre sous la forme

$$K_1 = R + R_1(xy) + R_2(xy)^2 + \ldots,$$

les R désignant des polaires de covariants indépendants des y.

24. A l'aide du covariant K, formons le nouveau covariant

$$\frac{\partial K}{\partial a_0} b_0 + \frac{\partial K}{\partial a_1} b_1 + \ldots + \frac{\partial K}{\partial a_n} b_n,$$

où nous pouvons remplacer les b par les coefficients de $(y_1 z_0 - z_1 y_0)^n$; nous trouvons alors le covariant

$$(26) \quad \frac{\partial K}{\partial a_n} y_1^n - \frac{\partial K}{\partial a_{n-1}} y_1^{n-1} y_0 + \frac{\partial K}{\partial a_{n-2}} y_1^{n-2} y_0^2 - \ldots \pm \frac{\partial K}{\partial a_0} y_0^n.$$

y_0 et y_1 ont été jusqu'ici regardés comme des constantes;

maintenant supposons-les variables, (26) est encore un covariant, car la relation $\mu = \Sigma ng - 2\nu$ est encore satisfaite; posons $K = A_x^\mu$ et remplaçons y par x, (26) deviendra le covariant déterminé par le semi-invariant $\frac{\partial A_0}{\partial a_n}$. La $r^{\text{ième}}$ polaire de ce covariant et (26) ont une différence divisible par (xy) (23).

On peut aussi prendre K égal à un invariant, (26) sera alors un covariant d'ordre n; si l'on pose dans ce covariant $y_1 = a$, $y_0 = -1$, on retrouve l'invariant, et en procédant ainsi on déduit toujours d'un invariant un covariant d'ordre n; au contraire, un covariant d'ordre n ne fournit pas toujours un invariant, le résultat pouvant parfois être identiquement nul; nous pouvons donner, sous une forme remarquable, la condition pour que les choses se passent ainsi. Si le covariant A_x^n est déduit de l'invariant J, (26) donne

$$A_0 = \frac{\partial J}{\partial a_n}, \qquad -nA_1 = \frac{\partial J}{\partial a_{n-1}}, \qquad \frac{n(n-1)}{1.2} A_2 = \frac{\partial J}{\partial a_{n-2}}, \qquad \ldots,$$

en sorte que

$$dJ = A_0\, da_n - nA_1\, da_{n-1} + \frac{n(n-1)}{1.2} A_2\, da_{n-2} - \ldots. \tag{27}$$

Un covariant d'ordre n détermine donc de cette manière un invariant quand le second membre de (27) est une différentielle exacte; si cela n'a pas lieu, on obtient un résultat identiquement nul.

25. Lorsque l'on a deux semi-invariants A_0 et B_0 la formule suivante en donne un nouveau

$$(A - B)^r = A_0 B_r - \frac{r}{1} A_1 B_{r-1} + \ldots,$$

pourvu cependant que r ne soit pas plus grand que l'ordre d'un des covariants déterminés par A_0 et B_0. Considérons la polaire $r^{\text{ième}}$ de l'un d'eux

$$A_x^{\mu-r} A_y^r$$

et posons dans cette polaire $x_0 = 0$, $x_1 = 1$, $y_0 = 1$, $y_1 = -B$;

nous obtiendrons le semi-invariant $(A - B)^r$ que nous appellerons le $r^{\text{ième}}$ *composant* de A et B.

Tout invariant est le $n^{\text{ième}}$ *composant de* a_0 *et d'un autre semi-invariant;* nous avons, en effet, trouvé

$$J = (A - a)^n, \qquad A_0 = \frac{\partial J}{\partial a_n}.$$

Ici, $(A - a)^{n-1}$ est identiquement nul; en effet, si, dans

$$A_0 a_{n-1} - \frac{n-1}{1} A_1 a_{n-2} + \frac{(n-1)(n-2)}{1.2} A_2 a_{n-3} - \ldots$$

on fait

$$A_0 = \frac{\partial J}{\partial a_n}, \qquad A_1 = -\frac{1}{n}\frac{\partial J}{\partial a_{n-1}}, \qquad \ldots,$$

le composant multiplié par n devient $\Delta_1 J$, c'est-à-dire zéro.

26. *Tout semi-invariant est une somme de composants de* a_0 *et de semi-invariants, dont le degré est moindre d'une unité.*

Dans

$$gH = \frac{\partial H}{\partial a_n} a_n + \frac{\partial H}{\partial a_{n-1}} a_{n-1} + \ldots + \frac{\partial H}{\partial a_0} a_0,$$

nous écrivons le second membre

$$A_0 a_n - \frac{n}{1} A' a_{n-1} + \frac{n(n-1)}{1.2} A'' a_{n-2} + \ldots,$$

où, d'après (24),

$$\Delta_1 A_0 = 0; \qquad \Delta_1 A' = A_0, \qquad \Delta_1 A'' = 2A', \qquad \ldots,$$

nous poserons

$$\begin{aligned} A' &= A_1 + B_0, \\ A'' &= A_2 + 2B_1 + C_0, \\ A''' &= A_3 + 3B_2 + 3C_1 + D_0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

$A_0, B_0, C_0, \ldots$ désignant des semi-invariants de degré $g - 1$.

On obtient alors

$$(28) \quad gH = (A - a)^n - \frac{n}{1}(B - a)^{n-1} + \frac{n(n-1)}{1.2}(C - a)^{n-2} + \ldots,$$

comme il est dit dans le théorème énoncé. Il est sous-entendu que les ordres de A_0, B_0, C_0, ... sont assez élevés pour que les compositions puissent être effectuées; tel n'est pas le cas lorsque le covariant dérivé de A_0 est d'un ordre inférieur à $2n$, les ordres de A_0, B_0, C_0, ... allant en diminuant de deux unités. Nous supposerons, par exemple, $D_0 = 0$, et nous supposerons que la formation de C_2 ne puisse pas être effectuée. (La difficulté se présente dans le dernier terme d'une des équations précédentes.) On a alors

$$A''' = A_3 + 3B_2 + 3C_1,$$
$$A^{\text{IV}} = A_4 + 4B_3 + 4K,$$

où K est à déterminer; or, de $\Delta_1 A^{\text{IV}} = 4A'''$, on tire

$$\Delta_1 K = 3C_1;$$

de ce que C_2 ne peut pas être formé, cela doit tenir à ce que $\Delta_2 C_1 = 0$, en sorte que C_1 est un semi-invariant de seconde espèce; il faut montrer qu'il n'existe pas de fonction entière K, telle que $\Delta_1 K$ soit un semi-invariant de seconde espèce. En d'autres termes, il faut montrer que l'équation $\Delta_2\Delta_1 u = 0$ ne peut être satisfaite que si $\Delta_1 u = 0$.

Supposons que u soit une solution, effectuons une permutation symétrique sur les indices; nous obtiendrons une nouvelle fonction u_1, et alors $\Delta_1\Delta_2 u_1 = 0$ et, par suite,

$$\Delta_2\Delta_1\Delta_2 u_1 = 0;$$

ce qui nous donne, pour la première équation, la nouvelle solution $\Delta_2 u_1$.

Soient g le degré, ν le poids de u, $\Delta_2 u_1$ sera de degré g et de poids $ng - \nu + 1$. Supposons que u soit celle des solutions de degré g qui a le plus petit poids, alors

$$\nu \leqq ng - \nu + 1 \qquad \text{ou} \qquad ng - 2\nu \geqq -1.$$

$\Delta_1 u$ est un semi-invariant de seconde espèce, et si μ désigne l'ordre du covariant correspondant

$$ng - 2\nu = -\mu - 2,$$

ce qui est en contradiction avec ce qui précède, puisque μ est positif ou nul. C_1 doit donc être nul, et le théorème est vrai dans tous les cas.

Nous avons alors à notre disposition un moyen pour former tous les semi-invariants; en effet, en composant a_0 avec lui-même on forme les semi-invariants du second degré; en composant ceux-ci avec a_0, on a les semi-invariants du troisième degré, et ainsi de suite.

Exemple : Avec $A_0 = c_2$, $n = 3$, on forme l'invariant [*voir* (21)]

$$R = 2(A - A)^2 = 4(A_0 A_2 - A_1^2) = 4(a_0 a_2 - a_1^2)(a_1 a_3 - a_2^2) - (a_0 a_3 - a_1 a_2)^2.$$

Pour $n = 4$, on a

$$12(A_0 A_2 - A_1^2) = 2(a_0 a_2 - a_1^2)(a_0 a_4 + 2a_1 a_3 - 3a_2^2) - 3(a_0 a_3 - a_1 a_2)^2,$$

ce qui est un semi-invariant du quatrième ordre (ordre du covariant correspondant).

Pour $n = 2q + 1$, on a $a_0^2 a_{2q+1}^2 + \dots$ et, en différentiant par rapport à a_{2q+1}, on a un semi-invariant

$$e_{2q+1} = a_0^2 a_{2q+1} + \dots,$$

Ces semi-invariants et ceux que nous avons appelés d_2, d_4, d_6, ... peuvent servir à exprimer tous les semi-invariants sous forme rationnelle, avec des dénominateurs qui sont des puissances de a_0, et l'on pourra obtenir ainsi, ordinairement, des puissances moins élevées de a_0 en dénominateur, que si l'on employait les c et les d.

27. Nous avons vu que tous les semi-invariants, multipliés par une puissance convenable de a_0, pouvaient s'exprimer en fonction entière des c, et, en faisant usage des d et des e,

nous avons vu que cette puissance de a_0 pouvait être abaissée; on peut se demander si, en introduisant de nouveaux semi-invariants, on peut parvenir à réduire ultérieurement cette puissance de a_0.

On peut enfin se demander s'il n'existe pas un nombre fini de semi-invariants d'une forme permettant d'exprimer sous forme entière tous les autres. C'est ce qui a lieu effectivement, et Gordan en a donné une démonstration très compliquée en considérant successivement tous les semi-invariants de degrés croissants, en écartant ceux qui peuvent s'exprimer en fonction d'autres de degrés moindres; nous ne parlerons pas de cette démonstration, mais renverrons à celle beaucoup plus simple de Hilbert (*Mathematische Annalen*, Bd. 33). Sylvester a donné, à l'aide de longs calculs, le nombre des semi-invariants nécessaires jusqu'à $n = 10$ (*American Journal*, Bd. 2). L'auteur du présent Traité a poussé les recherches de Hilbert plus loin (*Acta mathematica*, Bd. 15; *Theorie der regulären Graphs*) et a obtenu des résultats qui permettront peut-être de trouver directement les semi-invariants en fonction desquels on peut exprimer les autres. Nous exposerons ici un problème dont la solution sera nécessaire pour arriver à ce but.

Si l'on considère l'expression

$$P_1 = (x_1 - x_2)^{\alpha_1} (x_1 - x_3)^{\alpha_2} \ldots (x_{n-1} - x_n)^{\alpha_\mu},$$

où P_1 est de même degré par rapport à tous les x, et si l'on forme la somme ΣP relative aux valeurs que prend P quand on y permute les x, ce sera une fonction symétrique, qui est susceptible dans des cas particuliers de s'annuler identiquement. Le problème dont nous avons parlé a pour but de caractériser les expressions P_1 qui jouissent de cette propriété.

28. Le premier composant de A_0 et B_0 est

$$D_0 = (A - B)' = A_0 B_1 - B_0 A_1.$$

On l'appelle le *déterminant fonctionnel* de A_0 et B_0 (à proprement parler, c'est celui des covariants correspondants):

si l'on forme le déterminant fonctionnel de D_0 et d'un autre semi-invariant C_0, on a

$$D_0 C_1 - C_0 D_1 = A_0 B_1 C_1 - A_1 B_0 C_1 - A_1 B_1 C_0 + A_2 B_0 C_0$$
$$= \frac{1}{2}[B_0(A-C)^2 + C_0(A-B)^2 - A_0(B-C)^2],$$

ce qui permet d'exprimer le déterminant fonctionnel au moyen de formes d'un degré moindre.

Le produit de deux déterminants fonctionnels est donné par la formule

$$2(A_0 B_1 - B_0 A_1)(C_0 D_1 - D_0 C_1)$$
$$= - A_0 C_0 (B-D)^2 + A_0 D_0 (B-C)^2 + B_0 C_0 (A-D)^2 - B_0 D_0 (A-C)^2.$$

On appelle *forme hessienne* de A_0 la quantité $A_0 A_2 - A_1^2$, Le second composant de cette quantité et de A_0 est, si l'on suppose que A_0 détermine un covariant, d'ordre μ

$$(A_0 A_2 - A_1^2) A_2 - (A_0 A_3 - A_1 A_2) A_1$$
$$+ \frac{1}{4\mu - 10} A_0 [2 A_1 A_3 + (\mu - 3) A_0 A_4 - (\mu - 1) A_2^2] = \frac{\mu - 3}{4\mu - 10} A_0 D_4.$$

où D_4 est formé d'une manière analogue à d_4.

Systèmes généraux de formes jusqu'à $n = 4$.

29. Nous supposerons que nous n'ayons affaire qu'à une seule forme fondamentale de degré $n \leqq 4$, et nous déterminerons *le système de formes qui lui correspond,* c'est-à-dire les semi-invariants nécessaires et suffisants pour pouvoir exprimer tous les autres. Pour y parvenir, nous établirons le théorème suivant :

Si, dans un semi-invariant d'une forme a_x^n, nous remplaçons respectivement $a_0, a_1, a_2, \ldots, a_n$ par $0, a_0, 2a_1, \ldots, na_{n-1}$, nous obtenons un semi-invariant.

Un semi-invariant u peut se mettre sous la forme

$$u = A + B a_0,$$

A ne contenant pas a_0. Nous poserons

$$\Delta_1 u = a_0 \frac{\partial u}{\partial a_1} + \Delta'_1 u,$$

où

$$\Delta'_1 u = 2a_1 \frac{\partial u}{\partial a_2} + 3a_2 \frac{\partial u}{\partial a_3} + \ldots + n a_{n-1} \frac{\partial u}{\partial a_n};$$

et, comme $\Delta_1 u = 0$, on a

$$0 = a_0 \frac{\partial A}{\partial a_1} + \Delta'_1 A + a_0 \Delta_1 B,$$

où a_0 n'entre pas dans $\Delta'_1 A$; cette équation se partage alors dans les deux suivantes :

$$\frac{\partial A}{\partial a_1} + \Delta_1 B = 0, \qquad 2a_1 \frac{\partial A}{\partial a_2} + 3a_2 \frac{\partial A}{\partial a_3} + \ldots = 0.$$

Si dans A on met a_0 à la place de a_1, $2a_1$ à la place de a_2, etc., A se changera en A' et l'on aura

$$a_0 \frac{\partial A'}{\partial a_1} + 2a_1 \frac{\partial A'}{\partial a_2} + \ldots + (n-1) a_{n-2} \frac{\partial A'}{\partial a_{n-1}} = 0,$$

formule qui montre que A' est un semi-invariant de a_x^{n-1}. Si g et ν sont le degré et le poids de u, le degré g' et le poids ν' de A' seront

$$g' = g, \qquad \nu' = \nu - g.$$

On passe facilement de A' à A. Quand on connaît A, u n'est pas en général déterminé, B ne l'étant pas. Mais si l'on a $u_1 = A + B_1 a_0$, $u_2 = A + B_2 a_0$, on a

$$u_1 - u_2 = (B_1 - B_2) a_0,$$

$B_1 - B_2$ désignant un semi-invariant de degré $g - 1$.

30. Pour $n = 2$, on voit facilement que a_0 et c_2 constitue le système général de formes et que $a_0^\alpha c_2^\beta$ est la forme la plus générale d'un semi-invariant.

Si $n = 3$, nous allons voir que le système général de formes est

$$a_0, \qquad c_2 = a_0 a_2 - a_1^2, \qquad c_3 = a_0^2 a_3 - 3 a_0 a_1 a_2 + 2 a_1^3$$

et l'invariant

$$\mathrm{H} = \frac{c_3^2 + 4c_2^3}{a_0^2} = (a_0 a_3 - a_1 a_2)^2 - 4(a_0 a_2 - a_1^2)(a_1 a_3 - a_2^2).$$

On a les valeurs suivantes de A'

$$a_0^2, \quad a_0^3, \quad a_0^2 c_2.$$

Tous les A' qui peuvent être formés à l'aide des semi-invariants de a_x^3 appartenant à a_x^2, ils ont la forme $a_0^\alpha c_2^\beta$, mais ici α et β ne sont pas arbitraires, car pour u on a $3g \geqq 2\nu$ et pour A', par suite, $3g' \geqq 2(\nu' + g')$; d'où $g' \geqq 2\nu'$ ou $\alpha \geqq 2\beta$. Ils peuvent tous s'exprimer comme produits des trois semi-invariants trouvés, excepté si $\alpha = 2\beta + 1$. Ce cas ne peut pas se présenter, car u aurait la forme

$$u = a_1 \mathrm{H}^\beta + a_0 \mathrm{B},$$

d'où

$$0 = \Delta_1 u = a_0 \mathrm{H}^\beta + a_0 \Delta_1 \mathrm{B},$$

où

$$\Delta_1 \mathrm{B} = -\mathrm{H}^\beta,$$

ce qui est impossible (26).

Si nous considérons un u arbitraire, nous pouvons en déduire l'A' correspondant et l'exprimer sous forme entière à l'aide des trois A' spéciaux, et si l'on remplace ces A' par les semi-invariants H, c_2, c_3, on a u exprimé à l'aide de ces quantités à un terme près de la forme $a_0 u_1$ qu'il faut calculer de la même manière, ce qui prouve que si le théorème est vrai pour le degré $g - 1$, il l'est pour le degré g; il est donc démontré.

Si $n = 4$, nous allons prouver que le système général de formes est

$$a_0, \quad c_2, \quad c_3, \qquad i = a_0 a_4 - 4 a_1 a_3 + 3 a_2^2,$$

$$j = (a_0 a_2 - a_1^2) a_4 + 2 a_1 a_2 a_3 - a_2^3 - a_0 a_3^2 = \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix},$$

i et j désignant deux invariants. Les A' sont

$$a_0^2, \quad a_0^3, \quad c_2, \quad c_3,$$

et il faut prouver que tous les A' peuvent s'exprimer sous forme entière à l'aide de ceux-ci.

Nous trouvons, comme plus haut, $g' \geqq \nu'$; si l'on exprime A' en fonction des c et a_0 (14), a_0 ne peut entrer en dénominateur, car pour tout c le degré et le poids sont égaux : tout A' doit donc se composer de termes de la forme

$$a_0^\alpha c_2^\beta c_3^\gamma.$$

Si $\alpha > 1$, a_0^α peut s'exprimer à l'aide de a_0^2 et a_0^3, et nous avons seulement à examiner le cas où $A' = a_0 c_2^\beta c_3^\gamma$. Mais on peut voir que ce cas ne peut pas se présenter; en effet, on aurait

$$u = a_1 S + a_0 B,$$

où S est un semi-invariant de a_x^4; pour A', on a $g' = \nu' + 1$ et pour u, $2g = \nu + 1$, et pour B, $2g_2 = \nu_2$; c'est la condition pour que B soit un invariant, et nous voyons comme pour $n = 3$ que l'équation est impossible. Donc tous les A' peuvent s'exprimer à l'aide des 4 considérés plus haut; nous en concluons que le système de formes est composé de

$$a_0, \quad c_2, \quad c_3$$

et des invariants i et j.

Nous n'avons considéré que des semi-invariants de première espèce, mais ils peuvent servir à former tous les covariants.

31. La signification des covariants et des invariants consiste en ceci : en les égalant à zéro, on obtient les propriétés des formes qui restent les mêmes quand elles subissent des substitutions linéaires. Le discriminant exprime une semblable propriété et est un invariant; pour a_x^3, c'est la quantité H écrite plus haut. Nous allons chercher, comme exercice, la condition pour que les points racines de $a_x^4 = 0$, ou les zéros de a_x^4, forment une proportion harmonique ou une division harmo-

nique sur une droite, en les considérant comme des abscisses de points en ligne droite; cette propriété n'est pas altérée par une substitution linéaire, et nous pouvons supposer les abscisses de nos quatre points égales à 0, 1, ∞ et -1; alors l'équation a la forme

$$4\xi_1\xi_0(\xi_1^2-\xi_0^2)=0, \quad \text{où} \quad a_0=a_2=a_4=0, \quad a_1=1, \quad a_3=-1;$$

on trouve $j=0$, condition qui convient à toute équation du quatrième degré.

Pour former le discriminant de a_x^4, nous observerons qu'il est du douzième degré par rapport aux racines de $a_x^4=0$, a_q est de degré q par rapport à ces racines; le discriminant est alors un invariant de poids 12 et, par suite, de la forme $\alpha i^3+\beta j^2$, α et β désignant des constantes dont le rapport est à déterminer (si nous faisons abstraction d'un facteur commun); nous considérerons, pour cela, une équation simple de discriminant nul, par exemple

$$x_1^4-x_1^2x_0^2=0,$$

ou

$$a_0=1, \qquad a_1=0, \qquad a_2=-\frac{1}{6}, \qquad a_3=a_4=0,$$

$$i=3\left(\frac{1}{6}\right)^2, \qquad j=\left(\frac{1}{6}\right)^3,$$

ce qui donne pour le discriminant

$$i^3-27j^2.$$

Les covariants égaux à zéro fournissent des points qui sont liés aux points racines des formes fondamentales par des relations qui restent inaltérées par une substitution linéaire. Par exemple, les formes a_x^2 et b_x^2 ont pour semi-invariant $a_0b_1-b_0a_1$ et pour covariant correspondant

$$(a_0b_1-b_0a_1)x_1^2+(a_0b_2-b_0a_2)x_1x_0+(a_1b_2-b_1a_2)x_0^2;$$

les points racines de cette équation forment une division harmonique avec les points racines de chacune des formes a_x^2, b_x^2 (*voir* p. 164).

Formes quadratiques à plusieurs variables.

32. La forme la plus générale d'une forme quadratique à n variables est, en supposant $a_{kl}=a_{lk}$,

$$(1)\qquad f=a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2+\ldots+a_{nn}x_n^2=\Sigma a_{kl}x_kx_l;$$

elle sera transformée par une substitution linéaire générale si l'on fait

$$(2)\qquad \begin{cases} x_1=\alpha_{11}y_1+\alpha_{12}y_2+\ldots+\alpha_{1n}y_n,\\ x_2=\alpha_{21}y_1+\alpha_{22}y_2+\ldots+\alpha_{2n}y_n,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ x_n=\alpha_{n1}y_1+\alpha_{n2}y_2+\ldots+\alpha_{nn}y_n,\end{cases}$$

où le déterminant de la substitution $\Sigma\pm\alpha_{11}\alpha_{22}\ldots\alpha_{nn}$ n'est pas nul. Nous supposerons les a et les α réels.

Nous avons vu plus haut (p. 85) que f pouvait être ramené, et cela de plusieurs manières, à la forme

$$(3)\qquad f=A_1y_1^2+A_2y_2^2+\ldots+A_py_p^2,$$

es A étant réels et les y désignant des fonctions linéaires et homogènes des x; nous supposerons ces fonctions linéairement indépendantes les unes des autres; si cela n'avait pas lieu, on pourrait toujours remplacer un certain nombre des y par leurs valeurs en fonction des autres et effectuer de nouveau la décomposition en carrés; en tout cas $p\leqq n$.

33. *Si l'on ramène f de deux manières à la forme* (3), *dans les deux cas le nombre des termes sera le même.*

Supposons, en effet, que l'on ait identiquement

$$A_1y_1^2+A_2y_2^2+\ldots+A_py_p^2=B_1Y_1^2+B_2Y_2^2+\ldots+B_qY_q^2,$$

où $q>p$. Les y étant linéairement indépendants, nous pouvons exprimer x_1, x_2, ..., x_p en fonctions linéaires de y_1, y_2, ..., y_p et des autres x et porter leurs valeurs dans Y_1, Y_2, ..., Y_q, qui deviendront des fonctions de y_1, y_2, ..., y_p, x_{p+1}, ..., x_n. En différentiant la relation trouvée par rapport

à x_{p+1}, on obtiendrait une relation entre les Y qui serait linéaire, ce qui est contraire à nos hypothèses. Donc $q=p$.

Dans tous les cas, il y aura un même nombre de coefficients A *et* B *positifs et négatifs.*

Supposons $A_1, A_2, \ldots, A_r$ positifs, $B_1, B_2, \ldots, B_l$ négatifs, et les autres A négatifs, les autres B positifs; si le théorème n'est pas vrai, nous pouvons supposer $r+l<p$. Si l'on pose

$$y_1=y_2=\ldots=y_r=Y_1=Y_2=\ldots=Y_l=0,$$

on pourra de ces équations tirer un certain nombre des x en fonction des autres et porter leurs valeurs dans l'équation

$$A_1 y_1^2+A_2 y_2^2+\ldots=B_1 Y_1^2+B_2 Y_2^2\ldots.$$

Si tous les Y s'annulent, c'est qu'il existe entre eux des relations linéaires, ce qui est contraire à nos hypothèses; s'ils ne sont pas tous nuls, le second membre de l'équation précédente sera positif, tandis que le premier sera négatif ou nul, ce qui est absurde.

Substitutions orthogonales.

34. Il y a des substitutions linéaires qui changent l'expression

$$x_1^2+x_2^2+\ldots+x_n^2$$

en

$$y_1^2+y_2^2+\ldots+y_n^2;$$

on leur donne le nom de *substitutions orthogonales*. Il est facile de voir qu'elles satisfont aux relations

$$(4)\qquad \alpha_{1p}^2+\alpha_{2p}^2+\ldots+\alpha_{np}^2=1\qquad (p=1, 2, \ldots, n),$$

$$(5)\qquad \alpha_{1k}\alpha_{1l}+\alpha_{2k}\alpha_{2l}+\ldots+\alpha_{nk}\alpha_{nl}=0\qquad (k, l=1, 2, \ldots, n;\ k\gtrless l).$$

En vertu de ces équations, si l'on multiplie la première équation (2) par α_{1k}, la seconde par α_{2k}, ... et si on les ajoute, on a

$$(6)\qquad y_k=\alpha_{1k}x_1+\alpha_{2k}x_2+\ldots+\alpha_{nk}x_n\qquad (k=1, 2, \ldots, n),$$

et l'on reconnaît, en vertu de $y_1^2+y_2^2+\ldots=x_1^2+x_2^2+\ldots$ que cette substitution est encore orthogonale.

Pour $n=2$ et $n=3$, les substitutions orthogonales représentent des transformations de coordonnées rectangulaires sans changement d'origine.

35. Nous allons essayer de ramener f à la forme (3) au moyen d'une substitution orthogonale; nous supposerons le problème possible, quitte à le démontrer plus loin.

La formule

$$f=A_1y_1^2+A_2y_2^2+\ldots+A_ny_n^2 \tag{7}$$

donne

$$\frac{\partial f}{\partial x_i}=2\sum A_k y_k\frac{\partial y_k}{\partial x_i}.$$

Cette équation, étant identique, subsistera en remplaçant x_1, x_2, ..., x_n par α_{1k}, α_{2k}, ..., α_{nk}, valeurs annulant les y, excepté y_1 qu'elles rendent égal à un, et alors on aura

$$a_{i1}\alpha_{1k}+a_{i2}\alpha_{2k}+\ldots+a_{in}\alpha_{nk}=A_k\alpha_{ik}\qquad(i=1,2,\ldots,n)$$

ou

$$\left\{\begin{array}{l}(a_{11}-A_k)\alpha_{1k}+a_{12}\alpha_{2k}+\ldots+a_{1n}\alpha_{nk}=0,\\ a_{21}\alpha_{1k}+(a_{22}-A_k)\alpha_{2k}+\ldots+a_{2n}\alpha_{nk}=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\end{array}\right. \tag{8}$$

d'où nous tirons, en éliminant les α et en remplaçant A_k par s,

$$\varphi(s)=\begin{vmatrix}a_{11}-s & a_{12} & a_{13} & \ldots\\ a_{21} & a_{22}-s & a_{23} & \ldots\\ \ldots & \ldots\ldots & \ldots & \ldots\end{vmatrix}=0. \tag{9}$$

Si l'on permute circulairement A_1, A_2, ..., A_n et y_1, y_2, ..., y_n l'équation (7) ne change pas; les coefficients de (2) se permutent circulairement, tandis que les x et les a ne changent pas; dans (8) A_k est remplacé par A_{k+1} tandis que les a en (9) ne changent pas. L'équation (9) a donc pour racines A_1, A_2, ..., A_n.

Toutes ces racines sont réelles. — En effet, les coefficients de l'équation (9) sont, par hypothèse, réels; s'il y a des racines imaginaires, elles doivent être conjuguées deux à deux; soient A_k et A_l deux semblables racines; remplaçons dans (8) A_k par sa valeur, alors de ces équations et de (4) on pourra tirer $\alpha_{1k}, \alpha_{2k}, \ldots, \alpha_{nk}$, et comme dans les équations qui déterminent A_k il n'entre pas d'imaginaires, pour déterminer $\alpha_{1l}, \alpha_{2l}, \ldots, \alpha_{nl}$, il suffira de changer i en $-i$; il en résulte que α_{jk} et α_{jl} sont conjugués : leur produit est donc positif, ce qui est impossible en vertu de (5).

36. Lorsque l'on remplace A_k par sa valeur dans (8) le déterminant de ces équations s'annule et l'une de ces équations devient une conséquence des autres, et si nous désignons par $A_{1k}, A_{2k}, \ldots, A_{nk}$ les mineurs relatifs à la première ligne, nous avons

$$\frac{\alpha_{1k}}{A_{1k}} = \frac{\alpha_{2k}}{A_{2k}} = \ldots = \frac{\alpha_{nk}}{A_{nk}} = \frac{1}{\sqrt{A_{1k}^2 + A_{2k}^2 + \ldots + A_{nk}^2}},$$

où le dernier rapport est déterminé par (4). Les α ont donc des valeurs bien déterminées quand tous les A ne sont pas nuls; si tel était le cas, on pourrait faire usage d'une autre ligne. Enfin, si tous les mineurs étaient nuls, deux des équations (8) rentreraient dans les autres, une des quantités α pourrait être choisie arbitrairement (moindre que 1); dans ce cas on a $\varphi'(s) = 0$, et deux valeurs de s sont égales, car

$$\varphi'(s) = -\frac{\partial\varphi}{\partial(a_{11} - s)} - \frac{\partial\varphi}{\partial(a_{22} - s)} - \ldots$$

et tous les termes du second membre sont nuls, car les dérivées $\frac{\partial\varphi}{\partial(a_{ii} - s)}$ sont des mineurs du déterminant $\varphi(s)$. On verrait de même que si deux des quantités α peuvent être choisies arbitrairement $\varphi''(s) = 0$ et ainsi de suite.

Nous allons montrer maintenant que la substitution considérée est orthogonale et que l'équation (3) est satisfaite. En

effet, si A_k et A_l sont des racines distinctes, on a

$$a_{i1}\alpha_{1k}+a_{i2}\alpha_{2k}+\ldots+a_{in}\alpha_{nk}=A_k\alpha_{ik},$$
$$a_{i1}\alpha_{1l}+a_{i2}\alpha_{2l}+\ldots+a_{in}\alpha_{nl}=A_l\alpha_{il}.$$

Si l'on multiplie la première équation par α_{il}, la seconde par α_{ik} et si l'on retranche, on a

$$a_{i1}(\alpha_{1k}\alpha_{il}-\alpha_{1l}\alpha_{ik})+a_{i2}(\alpha_{2k}\alpha_{il}-\alpha_{2l}\alpha_{ik})\ldots=(A_k-A_l)\alpha_{ik}\alpha_{il};$$

si l'on fait $i=1, 2, \ldots, n$ et si l'on ajoute toutes les équations ainsi obtenues, on remarque que, en vertu de la relation $a_{mp}=a_{pm}$, tous les termes du premier membre se détruisent et l'on a

$$(A_k-A_l)(\alpha_{1k}\alpha_{1l}+\alpha_{2k}\alpha_{2l}+\ldots+\alpha_{nk}\alpha_{nl})=0,$$

de sorte que les équations (5) sont satisfaites, ainsi que les équations (4) qui ont été introduites pour achever de déterminer les α.

De ces équations il résulte que tous les termes de la forme $B_{lm}y_l y_m$, où l et m sont différents, s'évanouissent, en sorte que l'on a bien la relation (3).

Invariants.

37. Une substitution linéaire transforme $\Sigma a_{ij}x_i x_j$ en une autre $\Sigma b_{ij}y_i y_j$, avec d'autres coefficients. Toute fonction des coefficients qui, après la substitution, se trouve seulement multipliée par une puissance du déterminant de la substitution est ce que l'on appelle un *invariant*.

Quand on multiplie le déterminant de la substitution

$$D=\Sigma\pm\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}$$

par lui-même on obtient un nouveau déterminant dont l'élément général est

$$c_{kl}=\alpha_{1k}\alpha_{1l}+\alpha_{2k}\alpha_{2l}, \ldots, \alpha_{nk}\alpha_{nl}.$$

Si la substitution est orthogonale tous ces éléments sont

nuls, sauf ceux de la diagonale principale qui sont égaux à 1; le déterminant D est donc dans ce cas égal à ± 1.

Dans le cas général les valeurs des coefficients de la transformée sont données par la formule

$$b_{ij} = \Sigma a_{kl} \alpha_{ki} \alpha_{lj}.$$

Si l'on multiplie le déterminant

$$\Delta = \Sigma \pm a_{11} a_{22} \ldots a_{nn}$$

deux fois par D, on obtient le déterminant Δ où les a sont remplacés par des b; mais si l'on multiplie Δ par D^2 le terme général sera

$$a_{i1} c_{j1} + a_{i2} c_{j2} + \ldots + a_{in} c_{jn},$$

ce qui montre qu'après le changement des a en b, Δ est multiplié par D^2. Δ est donc un invariant; on lui donne le nom de *discriminant* de f.

$\varphi(s)$ devient égal à Δ quand on fait $s = 0$. Donc $\Delta = 0$ est la condition pour que f se décompose en $n - 1$ carrés: c'est là une propriété qui ne se trouve pas altérée, comme on l'a vu, par une substitution linéaire.

Lorsque l'on effectue une substitution orthogonale, les coefficients de $\varphi(s)$ ne sont pas altérés; pour le voir il suffit de considérer l'expression

$$f - s(x_1^2 + x_2^2 + \ldots + x_n^2).$$

dont le discriminant est $\varphi(s)$, quel que soit s, ce qui exige que tous les coefficients de $\varphi(s)$ restent les mêmes après la substitution orthogonale.

NOTE.

SUR L'ÉQUATION $x^n = 1$.

1. De l'équation

$$f(x) = x^n - 1 = 0, \tag{1}$$

nous écartons par la division tous les facteurs qui se trouvent dans des expressions de la même forme et de degré moindre. Nous obtiendrons alors une équation

$$\varphi_n(x) = 0, \tag{2}$$

dont les racines sont

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},$$

où k a toutes les valeurs moindres que n et premières à n, en nombre $\varphi(n)$. Ces racines sont les racines primitives de l'équation (1).

On peut former les polynomes $\varphi_n(x)$, successivement, en s'appuyant sur le théorème suivant, qu'on démontre facilement en ayant égard aux arguments des racines :

Si p est un nombre premier qui divise n, on a

$$\varphi_{np}(x) = \varphi_n(x^p), \tag{3}$$

mais, si p ne divise pas n,

$$\varphi_{np}(x) = \frac{\varphi_n(x^p)}{\varphi_n(x)}. \tag{4}$$

On trouve, par exemple,

$$\varphi_2(x) = x + 1, \qquad \varphi_3(x) = x^2 + x + 1, \qquad \varphi_6(x) = x^2 - x + 1,$$
$$\varphi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Les coefficients sont -1, 0, $+1$ jusqu'à $n = 105$, où l'on trouve un coefficient -2. Les équations sont réciproques.

On a
$$\varphi_p(1) = p,$$
et, par l'équation (3),
$$\varphi_{p^\alpha}(1) = p;$$
dans tous les autres cas, l'équation (4) montre qu'on a
$$\varphi_n(1) = 1.$$

2. Si α est une racine quelconque de l'équation (2), toutes les racines sont exprimées par α^k, où k est premier avec n. Si l'on élève toutes les racines à la puissance k, on obtient les mêmes racines dans un autre ordre, et l'équation $\varphi_n(x) = 0$ reste inaltérée.

Si $\varphi_n(x) = 0$ est réductible, elle se partagera en équations irréductibles de même degré.

Soient
$$\Psi_1(x) = 0, \qquad \Psi_2(x) = 0$$
deux des équations, α une racine de la première, α^k une racine de la seconde. Si l'on élève toutes les racines de $\Psi_1(x) = 0$ à la puissance k, on obtient une équation de même degré qui a une racine commune avec l'équation irréductible $\Psi_2(x) = 0$; donc elle a toutes les racines de $\Psi_2(x) = 0$; donc $\Psi_1(x)$ est au moins du même degré que $\Psi_2(x)$.

De la même manière, on voit que $\Psi_2(x)$ est au moins de même degré que $\Psi_1(x)$; donc les $\Psi(x)$ sont du même degré.

3. Cependant on peut prouver que $\varphi_n(x) = 0$ est irréductible. Ce théorème a été démontré pour la première fois par

Gauss pour le cas où $n = p$. Plus tard Eisenstein, Kronecker, Dedekind, etc. ont donné des démonstrations, dont la plus simple, due à Eisenstein, est donnée p. 110. Nous donnerons ici une démonstration nouvelle pour $n = p^\alpha$.

Comme $\varphi_{p^\alpha}(1) = p$, on doit avoir, abstraction faite du signe (2),

$$\Psi_1(1) = p, \qquad \Psi_2(1) = \Psi_3(1) \ldots = 1,$$

et alors

$$\frac{1}{p} = \frac{\Psi_2(1)}{\Psi_1(1)} = \frac{(1-\alpha_1^k)(1-\alpha_2^k)\ldots}{(1-\alpha_1)(1-\alpha_2)\ldots},$$

où $\alpha_1, \alpha_2, \ldots$ désignent les racines de $\Psi_1(x) = 0$; ici la fonction est une fonction entière et symétrique des racines de $\Psi_1(x) = 0$ et pour cette raison est égale à un nombre entier, les coefficients de $\Psi_1(x)$ étant des nombres entiers, le premier égal à 1. L'équation ne peut donc être réductible.

La démonstration du cas général a coûté bien du temps et de grands efforts, et les démonstrations que l'on en a données sont très compliquées. La plus simple est due à Arndt.

Nous exposerons ici une démonstration nouvelle que l'auteur a trouvée trop tard pour l'insérer à sa place dans ce Traité. Elle est fondée sur un théorème connu de Gauss, à savoir :

Si $f(x) = 0$ est une équation à coefficients entiers et si l'on forme l'équation $\varphi(x) = 0$, dont les racines sont les puissances $p^{\text{ième}}$ des racines de $f(x) = 0$ (p désignant un nombre premier), le polynome

$$f(x) - \varphi(x)$$

aura tous ses coefficients divisibles par p.

Nous allons maintenant donner notre démonstration.

Soit

$$\varphi_n(x) = \Psi_1(x)\,\Psi_2(x)\ldots;$$

les racines de $\Psi_2(x) = 0$ sont les $k^{\text{ièmes}}$ puissances des racines de $\Psi_1(x) = 0$. Soit $m > n$ un nombre plus grand que tout

nombre qui divise tous les coefficients d'un polynome

$$\Psi_i(x) - \Psi_j(x).$$

Soit

$$t = An + k,$$

où A est le produit de tous les nombres premiers jusqu'à m, excepté ceux qui divisent k. Comme $x^n = 1$, en élevant toutes les racines de $\Psi_1(x) = 0$ à la puissance t on obtient

$$\Psi_2(x) = 0.$$

Soit

$$t = P_1 P_2 P_3, \ldots,$$

où les P sont des nombres premiers; ils sont tous plus grands que m; en élevant les racines de Ψ_1 aux puissances P_1, P_2, P_3, ..., on ne peut pas dans tous les cas retrouver Ψ_1, parce que le produit t change Ψ_1 en Ψ_2. Alors au moins un des nombres, par exemple P_1, changera Ψ_1 en un autre Ψ, par exemple Ψ_3. Alors

$$\Psi_1(x) - \Psi_3(x)$$

serait divisible par P_1, ce qui est impossible, puisque $P_1 > m$.

FIN.

23024 Paris. — Impr. GAUTHIER-VILLARS ET FILS, quai des Grands Augustins, 55.







